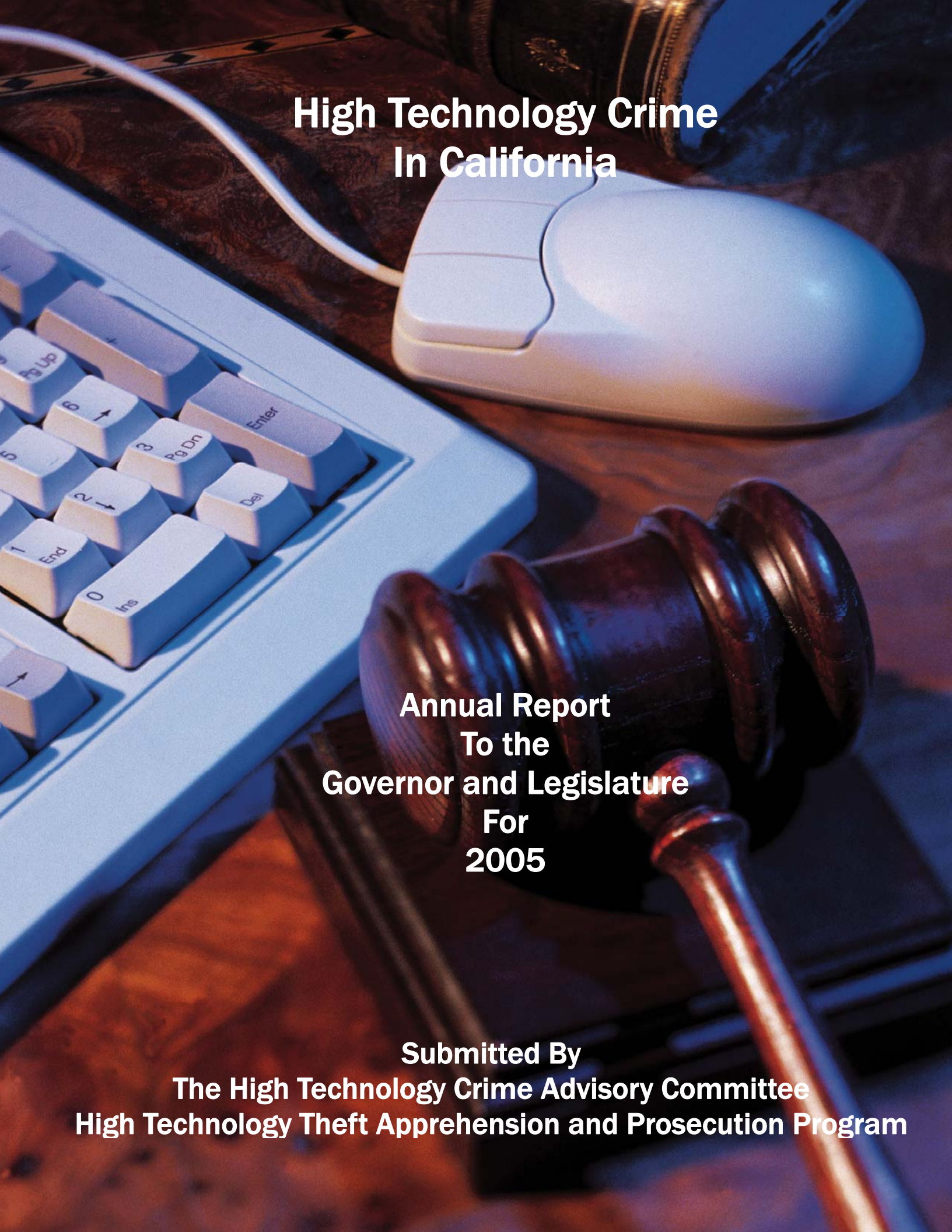


High Technology Crime In California

Annual Report To the Governor and Legislature For 2005

Submitted By
The High Technology Crime Advisory Committee
High Technology Theft Apprehension and Prosecution Program

December 2005

The Honorable Arnold Schwarzenegger
Governor of the State of California
Sacramento, CA 95814

The Honorable Don Perata
President Pro Tempore of the Senate
Sacramento, CA 95814

The Honorable Fabian Nuñez
Speaker of the Assembly
Sacramento, CA 95814

Dear Governor, Mr. President Pro Tempore, and Mr. Speaker:

High technology crime and identity theft continue to pose major threats to California—its citizens, its industries, and its enterprises. The annual losses suffered by California reach into the billions of dollars. These losses represent *direct losses* suffered by individual victims and corporations, and *indirect losses* resulting from lost wages, lost corporate profits, and lost tax revenues.

California has aggressively responded to the threats of high technology crime and identity theft through the High Technology Theft Apprehension and Prosecution (HTTAP) Program. The HTTAP Program is mandated by Section 13848 of the Penal Code. The HTTAP Program provides direction and funding through the Governor's Office of Emergency Services for five local high technology crimes task forces, five identity theft units, and three related support and training projects. Together, they comprise the California High Technology Crimes Task Forces.

By mandate of this statute, the HTTAP Program is overseen by a High Tech Crime Advisory Committee (HTCAC) which is responsible for developing a statewide strategy and priorities for addressing high technology crimes and identity theft. The HTCAC is required, on an annual basis, to review the effectiveness of the California High Technology Crimes Task Forces and report its finding to the Governor and Legislature. The attached report is submitted on behalf of the HTCAC in fulfillment of that requirement.

This report provides an overview of the HTTAP Program for Fiscal year 2004/05. The report also provides information on program accomplishments, recommendations, and funding.

It is our desire that this report provide you and your staff with valuable information that may assist you in formulating policy decisions concerning California's response to the threat of high technology crime.

Sincerely,

Clark Kelso, Chair
High Technology Crime Advisory Committee

Attachment

High Technology Crime in California

TABLE OF CONTENTS

	Page Number
Overview	4
New Laws	7
High Technology Crime Advisory Committee	13
Addressing the Problem of High Technology Crime	14
Addressing the Problem of Identity Theft	15
CDAA Prosecution Education	16
Department of Justice Activities	17
Conclusion	19
Northern California Computer Crimes Task Force (NC3TF)	21
Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)	26
Rapid Enforcement Allied Computer Team (REACT)	33
Southern California High Tech Task Force (SCHTTF)	38
Computer and Technology Crime High-Tech Response Team (CATCH)	42
Appendix A – California Penal Code Sections 13848-13848.8	49
Appendix B – High Technology Crime Advisory Committee Roster	58
Appendix C – Roster – Regional Task Forces – High Tech	63
Appendix D – Roster – Regional Task Forces – Identity Theft	64
Appendix E – Bylaws, Rules and Procedures of the High Technology Crime Advisory Committee	65

Overview

The astronomical growth rate of technology in the last ten years has brought numerous opportunities for economic development. It has also opened new windows of opportunity for crime. "Whether [technology] benefits us or injures us depends almost entirely on the fingers on the keyboard. So while the Information Age holds great promise, it falls, in part, upon law enforcement to ensure that users of networks do not become victims of New Age crime."[1] "It is the generally-accepted view of international, federal, state, and local law enforcement authorities that cyber crime, electronic crime, digital crime, or as many call it—*computer-related crime*—is a serious, growing issue."[2]

Computer-related crime continues to have a major impact on our nation, the state of California, and individual communities throughout California. Recent studies have shown that computer-related crime has grown exponentially since 1997, is costing billions of dollars in damages and losses, and is overwhelming law enforcement.[3] Criminals operating in cyberspace continually employ new techniques and new methods to commit crimes, thus making it more difficult for law enforcement to keep pace.

Recent statistics on computer-related crime show:

"Growth rates of computer security incidents…have very high growth curves, the incidents reported may represent only 5% of actual events, and one incident can impact thousands of systems and millions of users…"[4]

"Verifiable digital attacks worldwide caused economic damage…of more than $16 billion, almost double a year earlier. And 64% of digital attacks worldwide were against North American targets, compared to about 30% the previous year. Through 2005, 20% of companies are expected to experience serious (beyond virus) Internet security incidents."[5]

"…Almost 3.25 million Americans discovered that their personal information had been misused in this kind of fraud [identity theft] in the past year….Almost 10 million Americans have discovered that they were the victim of some form of identity theft within the last year."[6] In spite of these high numbers, "most victims of identity theft do not report the crime to criminal authorities…."[7]

[1] White House; "International Crime Control Strategy;" Washington, DC, 1998; 68.
[2] Joint Council on Information Age Crime; "Computer-Related Crime Impact: Measuring the Incidence and Cost;" January 2004; 5.
[3] Ibid; 4.
[4] Ibid; 7.
[5] Ibid; 8.
[6] Federal Trade Commission; "Identity Theft Survey Report; 2003; 4.
[7] Ibid; 9.

"The possession and distribution of child pornography is illegal under federal laws and in all 50 states; however…this crime is increasing and the increase is related to growing Internet use."[8]

A research report by the National Institute of Justice[9] breaks down computer-related crime into three basic categories:

- Crimes where the computer was used as a ***weapon*** for perpetrating the crime. This includes crimes where a computer was used to attack another system, acquire stored information, manufacture currency and checks, facilitate the acquisition of new identity information, etc.
- Crimes where the computer is the ***target*** of the crime. This includes crimes where a hacker has altered or destroyed information residing on a computer, engaged in a denial-of-service attack, compromised information stored on a computer, etc.
- Crimes where the computer is ***corollary*** to an offense as a storage medium. This would include crimes where the criminal has stored pertinent information on the computer such as financial ledgers used by drug dealers, child pornography, attack lists, etc.

Some common computer-related crimes include:

- Computer and network intrusions
- Computer hacking
- Internet-based stalking
- Terrorism and terrorist threats
- Internet-based threats of violence
- Software piracy
- Motion picture and recording piracy
- Denial of service attacks
- Theft of trade secrets
- Computer-related theft
- Technology-related theft
- Theft of high tech cargo
- Gray market-related illegal activity
- Internet-based financial crimes
- Telecommunications fraud
- E-scams
- Identity Theft

According to Edward J. Appel with the Joint Council on Information Age Crime, "The 'digital fingerprints' in crime scenes today can provide evidence as convincing as the

[8] U.S. Department of Justice, "Child-Pornography Possessors Arrested in Internet-Related Crimes; 2005; ix.
[9] U.S. Department of Justice; "Electronic Crime Needs Assessment for State and Local Law Enforcement," 2001; 9.

perpetrator's actual fingerprints or DNA." [10] However, law enforcement is struggling to cope with the steep rise in computer-related crime and digital evidence. These impacts include the high costs associated with cyber technologies, skills, training, investigation, analysis, and presentation of evidence.[11]

A study by the National Institute of Justice stressed the need for regional task forces to address the technically-challenging and time-consuming job of investigating crimes involving electronic evidence.[12]

The California High Technology Crimes Task Force strategy was created through Senate Bill 1734 in 1998 to help combat these types of crimes. This legislation established the High Technology Theft Apprehension and Prosecution (HTTAP) Program which is funded through the Governor's Office of Emergency Services (OES)[13]. Since 1998, the program has expanded to include five regional task forces within the state of California covering 30 counties. The mission of the HTTAP Program Task Force model is the investigation, apprehension, and prosecution of high technology crimes.

As multi-jurisdictional and multi-agency teams, each task force has the ability to cross borders which hinder local investigators not associated with a task force. Investigators are able to arrest and prosecute a wide range of criminal offenders and provide high technology-oriented service to the communities within the areas covered.

The HTTAP Program was expanded in 2001 to address the ever-growing problem of identity theft. Five additional task forces specializing in this arena were created to focus on combating identity theft in California. These identity theft task force units work in collaboration with the five original HTTAP High Tech task forces.

[10] Joint Council on Information Age Crime; "Computer-Related Crime Impact: Measuring the Incidence and Cost;" January 2004; 2.
[11] Ibid; 10.
[12] U.S. Department of Justice; "Electronic Crime Needs Assessment for State and Local Law Enforcement," 2001; x
[13] Originally funded through the Governor's Office of Criminal Justice Planning (OCJP). In December, 2003, OCJP was abolished as a separate state agency and was reorganized as the Criminal Justice Programs Division of the Governor's Office of Emergency Services (OES).

New Laws

The following bills dealing with high technology crimes (including identity theft) were recently introduced or will soon be enacted. A summary of each is shown below. For details on any pending California high technology legislation, please visit the web site for the California District Attorneys' Association at www.cdaa.org or send an email to High Tech Crimes Research Attorney Charles W. Barnes at cbarnes@cdaa.org.

AB 33 (Runner) – Internet Communication with Minor
Prohibits contacting a person 13 or under in order to lure them away for any purpose; punishable as a misdemeanor; provides for forfeiture of computers used in the offense.

AB 35 (Spitzer/Runner) – Sex Offender Registration/Megan's Law
Currently, personal identifying information for registered sex offenders in California is available online. The specific information made public for each registrant depends on the severity of the offense. Under this bill, every registrant's address, vehicle, and employment information would be available to the public.

AB 41 (Yee) – Child Sexual Exploitation
Trafficking in persons for forced labor or services is made a felony. It also creates a felony for trafficking a minor for sexual servitude and provides for various sentence enhancements and forfeiture provisions.

AB 64 (Cohn) – Intellectual Property/Piracy
Amendment to CA PC 653w. Advertising, manufacturing, or selling 100 or more audio or AV recordings without disclosing their manufacturer or other identifying information is chargeable as a misdemeanor or felony. (Currently, CA PC 653w is triggered by manufacture of 1,000 or more works.)

AB 278 (Bogh) – Identity Theft
Requires commercial mail receiving agencies to obtain users' thumbprints. Release of this information to law enforcement would occur only with showing of probable cause.

AB 281 (Liu) – Child Pornography
It is a misdemeanor or felony for a person to possess more than 100 items of child pornography. Expert witness testimony is not required at trial to prove that a depicted child is real.

AB 282 (Benoit) – Exhibiting sexually explicit materials
It is a misdemeanor to exhibit sexually explicit material in a motor vehicle so that it is open to public view.

AB 421 (Spitzer) – Privacy
It is a felony or misdemeanor to distribute--or aid in the distribution of--personal information about a person less than 18 years old with the knowledge that the information is to be used for a crime.

AB 424 (Calderon) – Identity Theft
Expands the definition of "personal identity information" to include any "equivalent form of identification." Expands the definition of "person" to include various types of business entities and other organizations.

AB 437 (Parra) – Child Exploitation/Megan's Law
Requires that the DOJ registered sex offender website include the date the crimes were committed and when the perpetrator is to be released.

AB 546 (Garcia) – Obscenity
Makes it illegal to use a state computer to download obscene material, apart from legitimate law enforcement needs.

AB 618 (Cogdill) – Identity Theft
Applies grand theft statutes to identity theft, and establishes enhanced penalties for persons found guilty of second violations of identity theft statutes.

AB 786 (Ruskin) – Identity Theft
Would provide a California State University (CSU) employee with four hours of paid time off following a disclosure by the university that there has been a breach of security involving the employee's personal identifying information.

AB 893 (Horton) – Child Exploitation/Parole
When a placement location is proposed for a sexually violent predator in the conditional release program, consideration shall be given to the age and profile of the offender's victim.

AB 916 (Canciamilla) – Identity Theft/Elder Abuse
Anyone who is convicted of felony violations of various elder abuse laws, including identity theft, shall receive sentence enhancements based on the loss to the victim.

AB 946 (Wyland) – Identity Theft
Increases fines imposed under CA PC 530.5.

AB 988 (Bogh) – Identity Theft/Criminal Profiteering
Adds 'identity theft' to crimes that may establish "criminal profiteering activity" under CA PC 186.2.

AB 1023 (Walters) – Child Exploitation/Child Pornography
All child pornography/exploitation crimes in which the victim is 14 or under would be mandatory felonies.

AB 1035 (Frommer) – Privacy/Public Officials
Prohibits knowingly posting an official's home address or phone number on the Internet and provides a civil remedy.

AB 1036 (Koretz) – Identity Theft
Adds the county where an identity theft victim lives to the jurisdiction where criminal action may be brought against the perpetrator.

AB 1069 (Montañez) – Identity Theft
Expands definition of "deceptive identification document." Prohibits possession of a document-making device with the intent to create, forge, or alter deceptive identification documents. Misdemeanor.

AB 1153 (La Suer) – Child Exploitation
Anyone 21 or older, who impersonates a minor in order to communicate with a child 12 or younger, with the intent to commit a sexual offense, is guilty of a misdemeanor.

AB 1257 (Umberg) – Child Exploitation
A first 'child pornography' offense is chargeable as a felony.

AB 1305 (Runner) – Privacy/Wiretaps
Redefines "wire communication" to exclude electronically stored communications.

AB 1323 (Vargas) – Registered Sex Offenders
Establishes a Department of Justice web page with information on sex offenders. Allows law enforcement to disseminate information on sex offenders as it sees fit, but prohibits others from publishing that information online.

AB 1527 (Liu) – Identity Theft
Prohibits a financial institution from issuing an account number if the same number was held by another customer in the preceding three years.

AB 1566 (Calderon) – Identity Theft
Marginally increases identity theft penalties when the victim is a member of the armed forces.

AB 1581 (Garcia) – Identity Theft
Makes it an alternative felony/misdemeanor to acquire, transfer, or retain the personal information of 100 or more persons with the intent to defraud.

AB 1595 (Evans) – Privacy
This bill prohibits the display, on the Internet, of the address or telephone number of any elected or appointed official when that official has made a written demand not to display such information.

AB 1694 (Leno) – Identity Theft
Requires credit reporting agencies to place (upon request and without charge) a security freeze on a consumer's credit report when the consumer's account has been breached. Requires notification of the consumer when a new application is made in the consumer's name, but under a different address.

SB 43 (Battin) – Megan's Law
Adds specified felony child pornography offenses and "annoying or molesting a child under the age of 18" to the Megan's Law Internet Web site. Allows the offender to request removal from the site if the victim was 16 or older.

SB 92 (Murray) – Spyware Penalties
Someone who has had "spyware" installed on his/her computer in violation of the law may bring an action for damages. Internet Service Providers (ISP's), the Attorney General, and a district attorney may also bring suit. This offense may also be punished as a misdemeanor.

SB 96 (Murray) – Copyright/Pornography/Peer-to-Peer Issues
It is illegal to promote or distribute peer-to-peer software, capable of sharing contraband files, unless the software incorporates available filtering technology to prevent such use. Exempts computer operating systems, Internet browser software, electronic mail service providers, ISPs, transmissions on LANs.

SB 97 (Murray) – SPAM
Makes use of fraudulent or misleading information in e-mail advertisements a misdemeanor.

SB 128 (Ackerman) – Identity Theft/Gangs
Offenses relating to theft of access cards and personal information are added to the list of offenses qualifying for a 'pattern of criminal gang activity.'

SB 222 (Runner) – Identity Theft/Privacy
Publicly posting someone's Social Security number is made a misdemeanor, as well as other acts which compromise the security of a Social Security number.

SB 277 (Battin) – Sex Offender Registration
Prohibits the placement of any sex offender parolee within 1-½ miles of any park, day care center, public or private school. Law enforcement must be notified 60 days prior to a sex offender's release.

SB 346 (Battin) – Identity Theft
Provides that a child, whose legal guardian has illegally used the child's identifying information, may become a dependent of the court.

SB 355 (Murray) – Internet Regulation/Phishing
Provides civil remedies against someone who, through electronic means, falsely purports to represent a business to induce another to disclose personal identifying information.

SB 444 (Ackerman) – Identity Theft
Various crimes related to identity theft and false identifications are added offenses that can establish a pattern of criminal gang activity.

SB 451 (Poochigian) – Identity Theft
Any application for a driver's license from the Department of Motor Vehicles (DMV) must require a thumbprint, fingerprint, or both, as determined by the department. The information collected under this bill would be used only to identify the applicant, determine his eligibility for a driver's license, and to investigate fraud related to the issuance of a driver's license.

SB 460 (Margett) – Identity Theft
Precludes any offender confined in a county facility or the Department of Corrections from performing work that gives them access to the personal identifying information of others.

SB 461 (Margett) – Child Pornography
Technical, nonsubstantive change.

SB 504 (Alquist) – Identity Theft
Prohibits commercial automotive dealers from issuing credit or providing financing without first getting a thumbprint and making a photocopy of the buyer's valid identification. Would permit a law enforcement officer to inspect and seize such information pursuant to a valid warrant.

SB 550 (Speier) – Identity Theft/Privacy
"California Data Broker Access and Accuracy Act of 2005"
Comprehensive bill regulating businesses that gather and sell consumer information.

SB 613 (Denham) – Child Exploitation
An attempt to distribute harmful materials to a minor with the intent to seduce is punishable under penal code sections governing criminal attempts.

SB 682 (Simitian) – Privacy
This bill imposes requirements on identifying documents which are issued by various public entities, and that can be read remotely. Unauthorized remote reading of a person's identifying document through radio waves is punishable as a misdemeanor.

SB 839 (Poochigian) – Identity Theft
"ID Theft Traffickers Act of 2005"
Every person who, with intent to defraud, sells, transfers, or conveys the personal information of another, or who illegally acquires the personal identifying information of four or more persons within 12 months, is guilty of grand theft, chargeable as a felony or misdemeanor. Provides sentence enhancements for offenders who commit felony violations of this act, or victimize persons under 18, elders, or members of the armed forces.

SB 852 (Bowen) – Identity Theft
Entities that do business in California, and which maintain computerized personal identifying information, are required to notify consumers when there is a breach of that information, whether or not the data was computerized when it was unlawfully acquired.

SB 1028 (Bowen) – Computer Assisted Remote Hunting
Prohibits Internet-assisted remote hunting.

High Technology Crime Advisory Committee

The High Technology Crime Advisory Committee was established concurrently with the HTTAP Program.[14] The purpose of the committee is to provide strategic oversight to the program and conduct planning in response to high technology crime in California. This committee includes representatives of the following agencies/organizations:

- A designee of the California District Attorneys' Association.
- A designee of the California State Sheriffs' Association.
- A designee of the California Police Chiefs' Association.
- A designee of the Attorney General.
- A designee of the California Highway Patrol.
- A designee of the High Tech Criminal Investigators' Association.
- A designee of the Governor's Office of Emergency Services.
- A designee of the American Electronic Association to represent California computer system manufacturers.
- A designee of the American Electronic Association to represent California computer software producers.
- A designee of the California Cellular Carriers' Association.
- A representative of the California Internet industry.
- A designee of Semiconductor Equipment and Materials International.
- A designee of the California Cable Television Association.
- A designee of the Motion Picture Association of America.
- A designee of either the California Telephone Association or the California Association of Long Distance Companies. This position shall rotate every other year between designees of the two associations.
- A representative of the California banking industry.
- A representative of the Office of Privacy Protection.
- A representative of the Department of Finance.
- A designee of the Recording Industry Association of America
- A designee of the Consumers Union.

[14] See Section 13848 of the California Penal Code.

Addressing the Problem of High Technology Crime

The HTTAP Program (through grants from OES) currently funds five regional task forces that comprise the California High Technology Crimes Task Force to address the growing problem of high technology crime. Refer to the back cover of this report for a geographical representation of the areas covered by each individual task force. Collectively, during the 2004-2005 fiscal year, these five task forces:

- Filed 552 cases involving high technology crimes
- Investigated 2,097 cases involving high technology crimes
- 15,588 victims were involved in the cases filed
- 395 convictions were obtained
- $305,914,885 in total aggregate monetary loss was suffered by the victims

A total of $9,868,000 was awarded to the five high technology crime task forces during this period. Each task force provided a 25 percent match, for a total funding of $12,335,000. This money was allocated collectively as follows:

- Personnel 72%
- Operating Expenses 25%
- Equipment 3%

For detailed information on statistics and funding by individual task force, please refer to each task force's section of this report.

Addressing the Problem of Identity Theft

As stated earlier in this report, the HTTAP Program also funds five regional identity theft units to combat the ever-growing crime of identity theft. Collectively, during the 2004-05 fiscal year, these five Identity Theft units:

- Filed 880 cases involving identity theft
- Investigated 3,579 cases involving identity theft
- 7,321 victims were involved in the cases filed
- 845 convictions were obtained
- $22,807,717 in aggregate monetary loss was suffered by the victims

A total of $2,850,000 was awarded to each of the five identity theft units during this period. Each identity theft unit provided a 25 percent match, for total funding of $3,562,500. This money was allocated collectively as follows:

- Personnel 64%
- Operating Expenses 32%
- Equipment 4%

California District Attorneys Association Activities

As part of the HTTAP Program, funds were allocated to the California District Attorneys' Association (CDAA) for the development and implementation of a statewide education and training program. This program assists local prosecutors in the efficient and effective prosecution of crimes perpetrated with the use of high technology.

The CDAA High Technology Theft Prosecution Education Program provides training to prosecutors, investigators, and law enforcement officers from all 58 counties in California. This training targets the successful investigation, apprehension, and prosecution of criminal organizations, networks, and groups of individuals involved in high technology and computer-based crimes. The cases involve computer-related or advanced technology issues, including white-collar crimes and identity theft.

In addition to providing training seminars, the program supports:

- Development and publication of the high technology crimes newsletter, *Firewall,* and a prosecution manual.
- Development and maintenance of online resources, including a brief bank and expert witness database.
- Provision of legal research services and other assistance as needed to California prosecutors and investigators.

A total of $312,500 was awarded to CDAA in furtherance of these activities.

California Department of Justice (DOJ) Activities

DOJ is actively involved in the HTTAP Program through three separate projects:

Department of Justice – Deputy Attorney General (DAG) Identity Theft Support
Department of Justice – Advanced Training Center
Department of Justice – Database

DOJ Deputy Attorney General – Identity Theft Support

Currently, five Deputy Attorneys General (DAGs) are assigned to the five regional task forces supported by the High Technology Identity Theft Program, administered through the Governor's Office of Emergency Services (OES). Funds have been allocated to DOJ to create the HTTAP-Identity Theft Support Project, which is part of the Special Crimes Unit in the Office of the Attorney General.

The DAGs also provide education and prosecution services to rural areas within California that are not currently served by the regional units. Additionally, the DAGs serve as points-of-contact for California law enforcement inquiries, and facilitate out-of-state identity theft-related inquiries.

A total of $450,000 was awarded to DOJ in furtherance of the DAG Identity Theft Support Project.

DOJ Advanced Training Center

The DOJ Advanced Training Center (ATC) has in place an interagency agreement with the Governor's Office of Emergency Services. The goals of this agreement are:

- To provide additional high technology investigation training classes to California peace officers, especially personnel assigned to the five regional task forces
- To provide advanced training in the area of computer forensics
- To provide equipment to personnel assigned to conduct computer forensic examinations.

The primary objectives are:

- To create a program that would continuously update the curriculum for teaching high technology investigation techniques and computer forensics.
- To base the changes on trends in crime, law and technology.
- To create a program (a series of classes) that would train an investigator, from a 'basic introduction' to high technology crimes, to an advanced level of computer forensic investigations competency.
- To develop the classes necessary to complete this series

- To test the students on learned skills and knowledge of computer crime investigations.

DOJ Database

"A total of $422,500 was awarded to DOJ in furtherance of the State Hi-Tech Crimes Database. Approximately $90,000 was returned to state coffers unused (monies designated to explore a data bridge). The remaining monies were spent on salaries, consultant expenses, maintenance, and new equipment. Attempts by LEA personnel to create a data bridge proved tenuous and the Database Committee voted to discontinue bridging efforts. Additionally, at the urging of the full committee, an examination of the database was commenced to determine true investigative usage. The results strongly confirmed that the database was not being utilized in a meaningful way."

Conclusion

The prevalence of electronic crimes, and the ability to investigate and prosecute them, are major concerns for California. A report by the National Institute of Justice (*Electornic Crime Needs Assessment for State and Local Law Enforcement*)[15] defined "the critical ten" for electronic crime investigations and prosecutions. These critical ten are:

1. Public awareness
2. Data and reporting
3. Uniform training and certification courses
4. Onsite management assistance for electronic crime units and task forces
5. Updated laws
6. Cooperation with the high-tech industry
7. Special research and publications
8. Management awareness and support
9. Investigative and forensic tools
10. Structuring a computer crime unit

California has made significant progress toward developing these "critical ten"; however, more effort is still needed.

High technology crime and identity theft continue to be major concerns for California. These types of crimes present unique challenges to law enforcement and the criminal justice system. High technology crimes and identity theft are often very different from traditional crimes—there is no physical crime scene, and there is often little, if any, physical interaction between victims, witnesses, and perpetrators. The crime is often discovered long after it was committed, and the collection of evidence requires training and expertise not readily found in local law enforcement agencies. Additionally, the prosecution of high technology criminals requires specialized expertise in order for the prosecutor to be able to adequately present the elements of the crime to the judge and jury while in the courtroom setting.

The task forces have received increasing numbers of requests for assistance from law enforcement agencies throughout California that do not have the equipment or the expertise to adequately respond to high technology crimes. Personnel shortages and staff turnover continue to compound the problem. The task forces rely upon highly-trained and qualified investigators provided by local agencies within their regions. These investigators are typically assigned to the task forces for two years. When their assignment is completed, new investigators are rotated into the positions, and valuable expertise is lost from the task forces.

[15] U.S. Department of Justice; "Electronic Crime Needs Assessment for State and Local Law Enforcement," 2001; 31.

Additionally, most task forces devote major portions of their grants to covering personnel costs. As personnel costs continue to rise and the grant amounts remain stable (or even decrease), the amount available for training, equipment, and new personnel decreases. This further taxes the task forces' abilities to respond to high technology crimes.

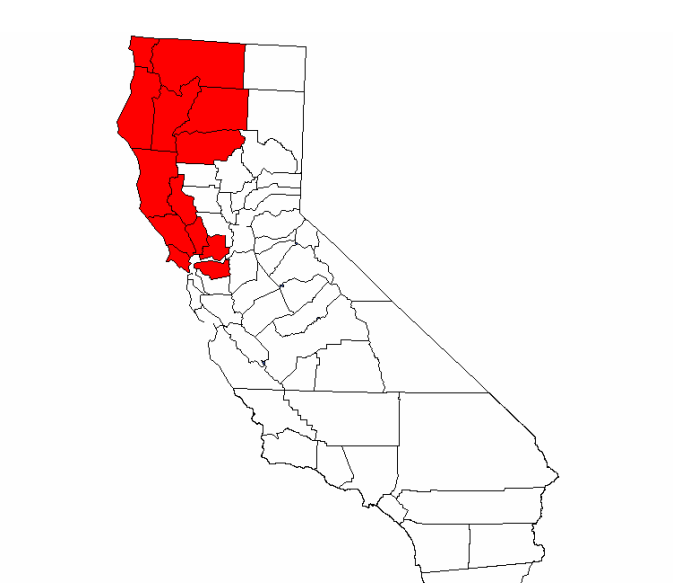
Finally, the HTTAP program currently represents approximately 30 counties in California. Law enforcement and prosecutorial agencies within the remaining counties must struggle to meet the demands of high technology crime investigations without the benefit of specialized task forces to investigate high technology crimes or identity theft.

In order to make an impact on high technology crimes and identity theft, additional funding is needed to address the increased costs associated with task force operations, and to address high technology crime and identity theft in counties that are not currently served by task forces.

Northern California Computer Crimes Task Force (NC^{3}TF)
Lead Agency: Marin County District Attorney's Office

NC^{3}TF is represented by the following thirteen counties:

- Contra Costa
- Del Norte
- Humboldt
- Lake
- Napa
- Marin
- Mendocino
- Shasta
- Siskiyou
- Solano
- Sonoma
- Tehama
- Trinity

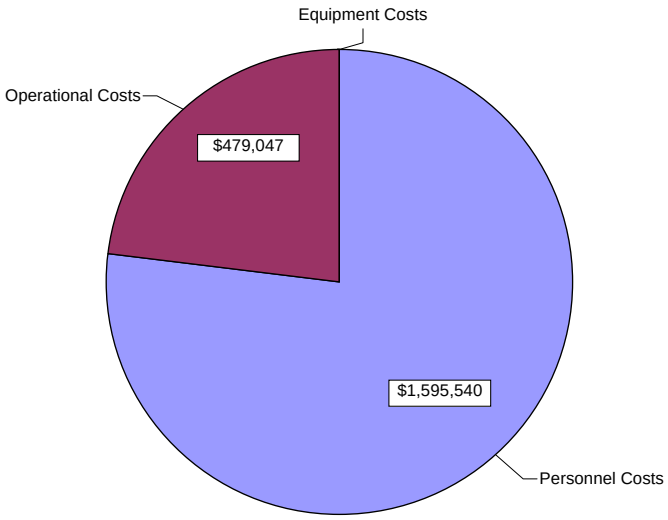


Through a memorandum of understanding, NC^{3}TF is comprised of participants from the following agencies:

- California Department of Justice; Bill Lockyer, Attorney General
- Concord Police Department; Ronald Ace, Chief
- Contra Costa County District Attorney; Robert Kochly, District Attorney
- Contra Costa County Sheriff's Department; Warren E. Rupf, Sheriff
- California Department of Motor Vehicles; Joan Borucki, Director
- Federal Bureau of Investigations;
- Humboldt County District Attorney; Paul Gallegos, District Attorney
- Lake County District Attorney; Gary Luck, District Attorney
- Marin County District Attorney; Paula Freschi Kamena, District Attorney
- Marin County Sheriff's Department; Robert T. Doyle, Sheriff
- Napa County District Attorney; Ed Berberian, District Attorney
- Napa County Sheriff's Department; Gary Simpson, Sheriff
- Novato Police Department; Chief Kreins
- Red Bluff Police Department; Al Shamblin, Chief of Police
- Redding Police Department; Leonard F. Moty, Chief of Police
- San Anselmo Police Department; Charles Maynard, Chief of Police

- San Pablo Police Department; Douglas Krathwohl, Chief
- San Rafael Police Department; John Rohrbacher, Acting Chief of Police
- Shasta County District Attorney; Gerald C. Benito, District Attorney
- Shasta County Sheriff's Office; Jim Pope, Sheriff-Coroner
- Siskiyou County Sheriff's Office; Rick Riggons, Sheriff-Coroner
- Solano County District Attorney; David W. Paulson, District Attorney
- Sonoma County District Attorney; Stephan R. Passalacqua, District Attorney
- United States Secret Service
- Vacaville Police Department; Warren Engelson, Acting Police Chief
- Vallejo Police Department; Robert Nichelini, Chief

NC^{3}TF – High Technology Crimes



During fiscal year 2004-05, NC^{3}TF received $1,973,600 in furtherance of the investigation of high technology crimes. NC^{3}TF provided a 25 percent match of these funds ($493,400) for a total grant award of $2,467,000. A breakdown of the budget categories is represented in the chart at the left.

During the grant period, NC^{3}TF expended 77 percent of its high technology grant budget on personnel costs, 23 percent on operational costs, and less than one percent on equipment costs.

During the grant reporting period, NC^{3}TF

- Filed 176 cases involving high technology crimes
- Investigated 489 cases involving high technology crimes
- 11,000 victims were involved in the cases filed
- 132 convictions were obtained
- $1,686,500 in total aggregate monetary loss was suffered by the victims

NC^{3}TF High Technology Case Highlights

Examples of cases investigated include:

NC3TF assisted the Napa Police Department on a nine-year-old homicide case involving a local dentist accused of murdering his wife during a domestic struggle.

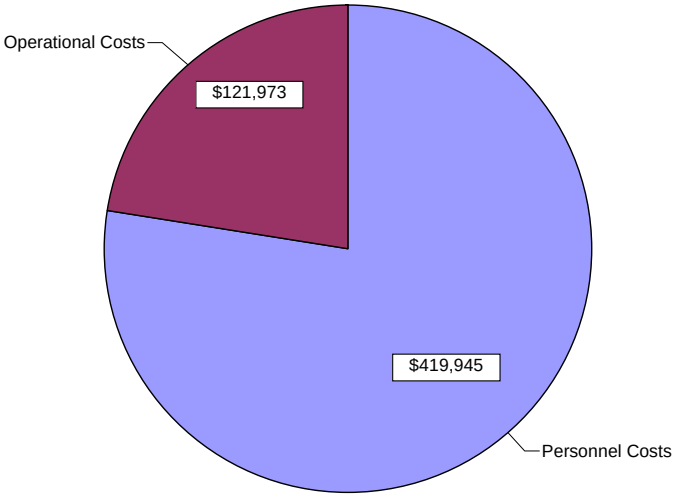
Although the case had never stopped being worked, advances in computer forensics and analysis--and the associated capabilities of the Task Force--played a key role in developing possible new evidence. NC3TF investigators worked with Napa Police detectives in serving a new search warrant and seizing ten computers for later analysis.

A 30-year-old Napa resident came to the attention of NC3TF via a "Cyber-Tip" received by the Vallejo Police Department from the "National Center for Missing and Exploited Children". Initial information revealed that the suspect was uploading images of child pornography to an Internet website. The subsequent joint investigation, initiated by NC3TF with Napa PD, revealed a very disturbing history and prior related cases. Numerous images of child pornography were discovered on the suspect's home computer. The suspect allegedly committed lewd acts on a nine-year-old female at his residence, along with several other underage females via the Internet. The suspect also solicited several adults (via the Internet) to commit sexual assaults upon their own children. Further, the suspect induced several underage females to expose themselves during Internet chat room conversations. The crimes were found to have occurred between 2002 and 2005. He was arrested at his residence in June, charged with twenty criminal offenses, and is being held on $500,000 bail.

Finally, the NC3TF has increased its exposure via multiple newspaper articles, television segments, and an especially productive June, 2005, live radio segment on AM radio station KSFO in San Francisco. Operations Manager Rick Nichelman used a local contact to coordinate a live discussion on Identity Theft and Internet crimes against children. Radio hosts Brian Sussman and Tom Benner queried Nichelman for over 20 minutes, and the very positive feedback may lead to the development of a regular question-and-answer segment on the morning talk show.

NC^{3}TF – Identity Theft Crimes

During fiscal year 2004-05, NC^{3}TF received $570,000 in furtherance of the investigation of identity theft crimes. NC^{3}TF provided a 25 percent match of these funds ($142,500) for a total grant award of $712,500. A breakdown of the budget categories is represented in the chart to the right.



During the grant period, NC^{3}TF expended 61 percent of its identity theft grant budget on personnel costs, 23 percent on operational costs, and 16 percent on equipment costs.

During the grant reporting period, NC^{3}TF

- Filed 56 cases involving identity theft crimes
- Investigated 235 cases involving identity theft crimes
- 842 victims were involved in the cases filed
- 29 convictions were obtained
- $465,000 in total aggregate monetary loss was suffered by the victims.

NC^{3}TF Identity Theft Case Highlights

Examples of cases investigated include:

Postal Service Inspector Bob Lieske and Investigator Mike Parsons are investigating a 41-year old Vallejo woman who was arrested in February of this year by the Contra Costa County Sheriff's Department. The suspect had been involved in a nine-county identity theft ring for approximately 18 months. She had fraudulently obtained credit cards by using the personal information from 15 victims. She had entered over 25 different businesses throughout Northern California and Nevada and was captured on surveillance tapes conducting many of these transactions. The suspect was also utilizing counterfeit California drivers' licenses with her photo and the personal information of her victims to accomplish the identity theft. To date, her illegally purchased goods are valued at $232,000. This case is ongoing, and the suspect is currently facing 147 counts with a maximum exposure of 100 years.

A second case involved NC3TF's intern program and Investigator Jemy Dinov, the Concord Police Department, and the Department of Motor Vehicles. In late 2004, a 37-year-old Richmond man (who was a wanted parolee from Contra Costa County) entered a Chevrolet dealership in Hayward. He purchased a $37,000 Chevy Monte Carlo, using the personal credit information of another person and a fraudulent California driver's license. With the success of this transaction, he next purchased a $30,000 Dodge Magnum from a dealership in Concord (with another fraudulent California driver's license and credit information of a second victim). Search warrants were served at his residence, and an arrest was made by the Concord Police.

During this five-month investigation, it was discovered that the suspect had obtained credit in several victims' names at various jewelry stores in the Bay Area, with a loss of $15,000. The suspect had in his possession the drivers' licenses from three victims, with his photograph and their personal information. One driver's license was an alias created by the suspect; the Department of Motor Vehicles determined that he had committed perjury to obtain this license. The Dodge Magnum was recovered by Concord Police Department, and Investigator Dinov recovered the Monte Carlo. There were three subsequent arrests in this case, and $67,000 in property was recovered. Deputy Attorney General Keith Lyon has assumed prosecution of the case. This case stands out a as a collaborative endeavor between several law enforcement agencies in the NC3TF region.

NC^{3}TF Steering Committee

NC^{3}TF receives direction and oversight from a local Steering Committee, comprised of representatives from the local high technology and financial industries, and of representatives from allied agencies associated with NC^{3}TF. The Steering Committee meets quarterly, at a minimum. The following agencies are represented on the NC^{3}TF Steering Committee:

- Lucas Films Ltd.
- Marin County District Attorney
- Napa County District Attorney
- Napa County Sheriff's Office
- Solano County District Attorney
- Sonoma County District Attorney
- Vallejo Police Department
- Wells Fargo Bank

Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)

Lead Agency: Sacramento Sheriff's Department

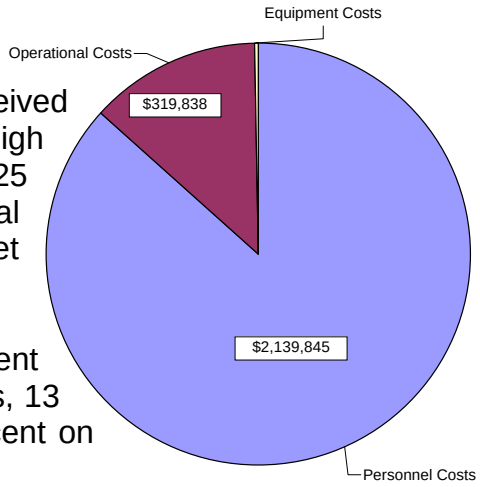
SVHTCTF is represented by the following seven counties:

- El Dorado
- Merced
- Placer
- Sacramento
- San Joaquin
- Stanislaus
- Yolo

Through a memorandum of understanding, the SVHTCTF is comprised of participants from the following agencies:

- California Department of Insurance; John Garamendi, Insurance Commissioner
- California Department of Justice; Bill Lockyer, Attorney General
- California Department of Motor Vehicles; Joan Borucki, Director
- California Highway Patrol; Mike Brown, Commissioner
- California State Controller's Office; Steve Westly, California State Controller
- Ceres Police Department; Art deWerk, Chief
- Davis Police Department; Jim Hyde, Chief
- El Dorado County District Attorney; Gary Lacy, El Dorado County DA
- El Dorado County Sheriff's Department; Jeff Neves, Sheriff
- Federal Bureau of Investigations; Drew Parenti, Special Agent in Charge
- Folsom Police Department; Sam Spiegel, Chief
- Isleton Police Department; Shane Diller, Chief
- Merced Sheriff's Department; Mark N. Pazin, Sheriff/Coroner
- Modesto Police Department; Roy W. Wasden, Chief
- Placer County District Attorney; Bradford R. Fenocchio, District Attorney
- Sacramento County Probation Department; Vern Speirs, Chief Probation Officer
- Sacramento County District Attorney; Jan Scully, District Attorney
- Sacramento Police Department; Albert Najera, Chief
- Sacramento Sheriff's Department; Lou Blanas, Sheriff
- San Joaquin Sheriff's Department; Baxter Dunn, Sheriff
- Stanislaus County District Attorney; Jim Brazelton, District Attorney
- Stanislaus Sheriff's Department; Les Weidman, Sheriff
- Turlock Police Department; Lonald D. Lott, Chief
- U.S. Attorney's Office; McGregor W. Scott, United States Attorney
- U.S. Postal Inspection Services; Lee Heath, Chief Postal Inspector
- U.S. Secret Service; Brady J. Mills, Assistant Special Agent in Charge
- University of California, Davis, Police Department; Calvin E. Handy, Chief
- USDA Forest Service; Gil Quintana, Special Agent in Charge
- Yolo County District Attorney; David C. Henderson, District Attorney

SVHTCTF – High Technology Crimes



During fiscal year 2004-05, the SVHTCTF received $1,973,600 for furtherance of the investigation of high technology crimes. The SVHTCTF provided a 25 percent match of these funds ($493,400) for a total grant award of $2,467,000. A breakdown of the budget categories is represented in the pie chart to the right.

During the grant period, SVHTCTF expended 87 percent of its high technology grant budget on personnel costs, 13 percent on operational costs, and less than one percent on equipment costs.

During the grant reporting period, SVHTCTF

- Filed 209 cases involving high technology crimes
- Investigated 529 cases involving high technology crimes
- 649 victims were involved in the cases filed
- 123 convictions were obtained
- $808,197.65 in total aggregate monetary loss was suffered by the victims.

SVHTCTF High Technology Case Highlights

Theft of Trade Secrets

The Task Force was contacted by Grass Valley Police Department regarding information they received from the Chief Executive Officer of a local technology business. The CEO described a sequence of events involving the disappearance of 10-15 binders containing notes and information kept by the Chief Operations Officer, which covered his three and a half years with the company, and contained information related to the company's sales, engineering, customers, and patent processes. According to the company, the technology (involving the breakdown and recombination of urethane foam) was valued at millions of dollars. Investigators learned that the suspect had resigned his position with the company, put his house up for sale, hired a moving company, and obtained airline tickets for himself and his family for the United Kingdom. Search warrants were obtained and executed at several locations. The evidence seized was examined by the Chief Executive Officer of the company. The Chairman of the Board and the Chief Executive Officer declined to proceed with formal prosecution based upon the evidence seized.

Status: Closed

Computer Crime (Hacking)

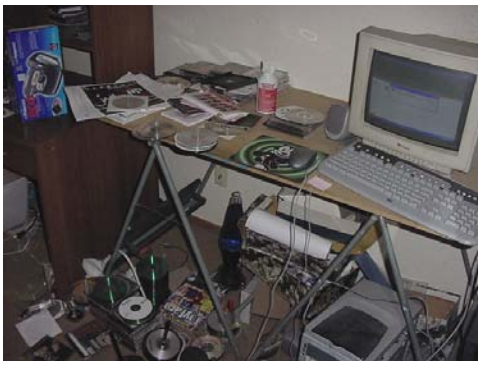
The Task Force was contacted regarding the "hacking" of Natomas High School's Student Information System computer database by at least two students. These students attempted to changes grades, and deleted more than 18,000 school records. The students also caused the "crash" of the student database on at least two occasions. Warrants were obtained for two residences where the students lived and evidence was seized.

Status: Ongoing investigation

Computer Crime (Hacking)

Detectives are currently investigating Sheldon High School students involved in hacking into the school's computer system, and the Elk Grove Unified School District's computer system. The investigation and forensic examination of three towers, two laptops and a key logger, revealed three suspects, the use of a "Cain and Abel" program, and a hacking tool. The suspects accessed the school's system to change grades and disciplinary records by keystroke logging and password cracking.

Status: Three arrests warrants pending D.A. review
Aggregate Loss: $10,000 minimum



Piracy

A suspect was found with a storage facility full of pirated DVDs. Additional follow-up by detectives resulted in the arrest of the suspect and the additional recovery of counterfeit DVDs, a seller's list, and a video camera.

Status: Arrested
Aggregate Loss: Undetermined

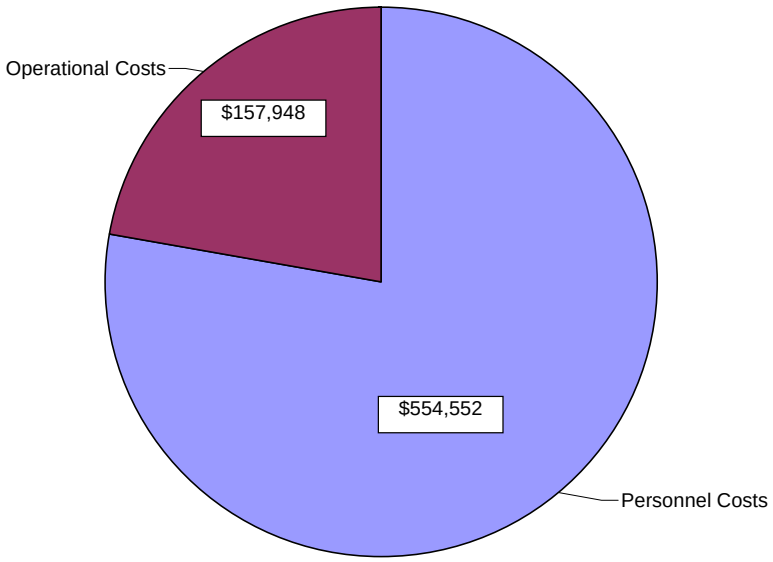
Possession of Stolen Property

Task Force detectives investigated a case where the suspect sold four stolen cable boxes on eBay. The detective recovered eight stolen Comcast cable boxes valued at $2,500, and obtained the suspect's confession. The suspect was arrested this month and booked into custody without incident.

Possession and Distribution of Child Pornography

Detectives received several NCMEC "CyberTip" reports regarding the possession and distribution of child pornography by a suspect whose ISP was listed as Yahoo. Search warrants were obtained for suspect information from Yahoo and SBC. Detectives went to the suspect residence and positively identified him. He admitting to the possession and distribution of child pornography and wrote an apology letter for what he had done. A search warrant was obtained for his computer, which revealed several thousand images of child pornography and a large quantity of movie files depicting children engaged in sexually-explicit conduct. The suspect was arrested.

SVHTCTF – Identity Theft Crimes



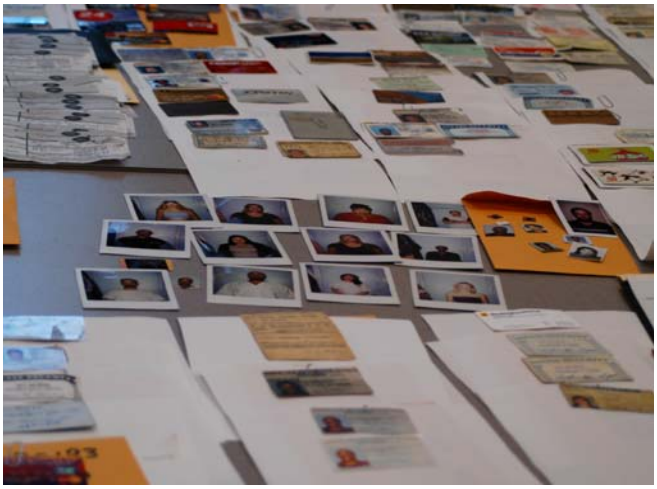
During fiscal year 2004-05, the SVHTCTF received $653,500 in furtherance of the investigation of identity theft crimes. Sacramento County Sheriff's Department provided a 25 percent match of these funds ($163,375) for a total grant award of $816,875. A breakdown of the budget categories is represented in the chart at the left

During the grant period, SVHTCTF expended 78 percent of its identity theft grant budget on personnel costs, 22 percent on operational costs, and nothing on equipment costs.

During the grant reporting period, SVHTCTF

- Filed 375 cases involving identity theft crimes
- Investigated 1,904 cases involving identity theft crimes
- 2,730 victims were involved in the cases filed
- 218 convictions were obtained
- $7,058,232.96 in total aggregate monetary loss was suffered by the victims.

SVHTCTF Identity Theft Case Highlights



Examples of cases investigated include:

Case #1
Three suspects attempted to cash several checks on the victim business account.
Status: 3 Arrested
Aggregate Loss: $20,000.00

Case #2
The suspect purchased a car on a blocked account and used the victim's Social Security number to apply for credit.
Status: Arrested
Aggregate Loss: $100,000.00

Case #3
Two suspects used a 19-year-old female to cash counterfeit checks totaling more than $32,500. The female was an employee of one of the suspects, and the other suspect was the person who produced and delivered the checks to the female. One of the suspects drove the female to various bank locations to cash the checks. The other suspect kept all of the money from the bogus checks.

Status: 2 Arrested
Aggregate Loss: $32,500.00

Case #4
The suspect entered the victim business and passed an altered check drawn on a bank account in the name of another. The suspect was arrested by store security and the Task Force was called. The suspect was found to be in possession of two additional altered checks (one completed, one incomplete). DMV records indicate the person whose name is shown on the check is deceased.

Status: Arrested

SVHTCTF Steering Committee

SVHTCTF receives direction and oversight from a local Steering Committee comprised of representatives from the local high technology and financial industries, and representatives from allied agencies associated with SVHTCTF. The Steering Committee meets, at a minimum, quarterly. The following agencies are represented on the SVHTCTF Steering Committee:

- American Network Services
- Apple Computer
- AT&T Wireless
- California Department of Insurance
- California Department of Justice
- California Department of Motor Vehicles
- California District Attorneys' Association
- California Highway Patrol
- California State Controller
- Ceres Police
- Comcast Cable
- Davis Police
- DHL/Airborne Express
- DIRECTV
- E*Trade Financial
- El Dorado County Sheriff
- Federal Bureau of Investigation
- Federal Express
- Folsom Police
- Hewlett-Packard
- Intel Corporation
- Isleton Police
- Merced Police
- Modesto Police
- Motion Picture Association of America, Inc.
- NEC Electronics
- Oracle
- Placer County District Attorney
- Placer County Sheriff
- Recording Industry Association of America

- Roseville Police
- Sacramento District Attorney
- Sacramento Police
- Sacramento County Probation
- Sacramento County Sheriff
- San Joaquin County Sheriff
- SBC
- Stanislaus District Attorney
- Stanislaus Sheriff
- Systems Integration Solutions, Inc.
- Tuolumne County Sheriff
- Turlock Police Services
- University of California, Davis, Police
- United Parcel Service
- United States Attorney’s Office
- United States Postal Inspection
- United States Secret Service
- USDA – Forest Service
- Verizon Wireless
- Wells Fargo Bank
- Yolo County District Attorney

Rapid Enforcement Allied Computer Team (REACT)
Lead Agency: Santa Clara District Attorney's Office

REACT is represented by the following five counties:

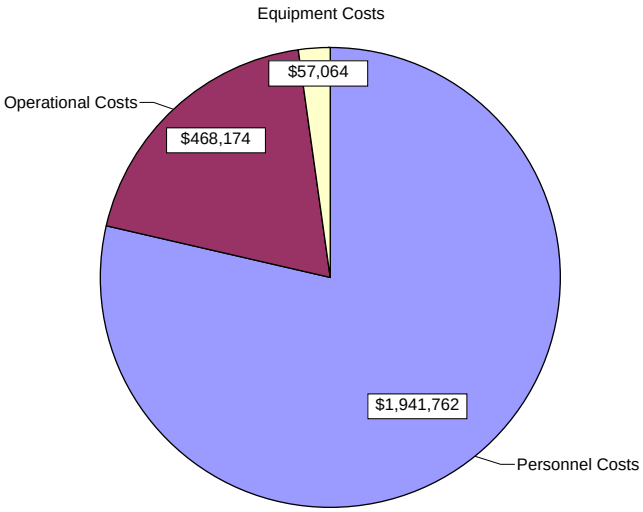
- Alameda
- San Francisco
- San Mateo
- Santa Clara
- Santa Cruz

Through a memorandum of understanding, REACT is comprised of participants from the following agencies:

- Alameda County District Attorney
- California Department of Justice
- California Highway Patrol
- Federal Bureau of Investigation
- Fremont Police Department
- Hayward Police Department
- Internal Revenue Service
- Menlo Park Police Department
- Mountain View Police Department
- Pacifica Police Department
- San Bruno Police Department
- San Francisco District Attorney
- San Francisco Police Department
- San Jose Police Department
- San Mateo County District Attorney
- San Mateo County Probation Department
- San Mateo County Sheriff's Office
- Santa Clara County District Attorney's Office
- Santa Clara County Sheriff's Office
- Santa Clara Police Department
- Santa Cruz County District Attorney
- Santa Cruz County Sheriff's Office
- South San Francisco Police Department
- United States Customs Service

REACT – High Technology Crimes

During fiscal year 2004-05, REACT received $1,973,600 in furtherance of the investigation of high technology crimes. REACT provided a 25 percent match of these funds ($493,400) for a total grant award of $2,467,000. A breakdown of the budget categories is represented in the chart to the right.



During the grant period, REACT expended 79 percent of its high technology grant budget on personnel costs, 19 percent on operational costs, and 2 percent on equipment costs.

During the grant reporting period, REACT

- Filed 37 cases involving high technology crimes
- Investigated 762 cases involving high technology crimes
- 456 victims were involved in the cases filed
- 35 convictions were obtained
- $245 million in total aggregate monetary loss was suffered by the victims.

REACT High Technology Case Highlights

Examples of cases investigated include:

Jerome Heckenkamp

In 1999 (prior to detailed collection of case statistics), REACT assisted the FBI with the arrest of Jerome Heckenkamp. Heckenkamp was responsible for the widely-publicized hacking and defacement of eBay, Amazon and over 300 other companies nationwide. In July of this year, Heckenkamp pled guilty to three counts of 18 USC 1030.

Costco Card Fraud

REACT agents were investigating the sale and failed delivery of $8,100 in $100 Costco cash cards via eBay when they uncovered a money-laundering scheme involving more than $500,000 in Costco cash cards. The case remains under investigation by REACT and the FBI's money laundering unit.

Theft, Internet Bank Fraud and Money Laundering

A suspect infiltrated numerous high tech retail firms and set up elaborate "bust-out" schemes involving complicit insiders. Large purchases were fraudulently authorized, shipped to drop locations, and then resold internationally. The proceeds were laundered through internet banking transactions, wire transfers, and cashiers' checks. Estimated losses exceed $10,000,000.

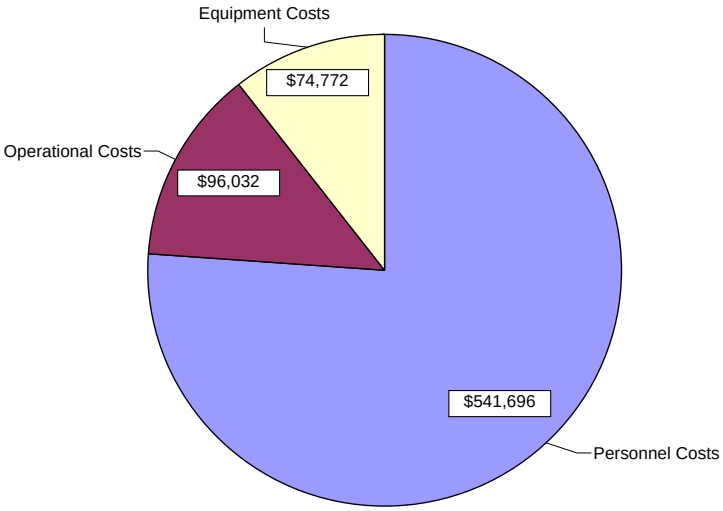
Fraudulent Destruct Contracts

A cooperative witness from a previous REACT investigation and prosecution alerted agents to a major theft/fraud involving certified destruction contracts. Local companies hired to destroy product from numerous large electronics manufacturers were operating in cooperation with high-end fences in the secondary market to divert the product back into circulation, while providing false certificates of destruction. Estimated losses from this scheme exceed $25,000,000.

Movie/Music Piracy

This quarter, REACT filed the first case in Northern California under Penal Code section 653z, which makes it illegal to operate a recording device in a movie theatre.

REACT – Identity Theft Crimes



During fiscal year 2004-05, REACT received $653,500 in furtherance of the investigation of identity theft crimes. REACT provided a 25 percent match of these funds ($163,375) for a total grant award of $816,875. A breakdown of the budget categories is represented in the chart to the left.

During the grant period, REACT expended 76 percent of its identity theft grant budget on personnel costs, 13 percent on operational costs, and 10 percent on equipment costs.

During the grant reporting period, REACT

- Filed 117 cases involving identity theft crimes
- Investigated 231 cases involving identity theft crimes
- 456 victims were involved in the cases filed
- 364 convictions were obtained
- $11 million in total aggregate monetary loss was suffered by the victims.

REACT Identity Theft Case Highlights

Examples of cases investigated include:

Lexis-Nexis

A REACT agent, assisting Hayward Police Department in a probation search, observed a stack of “Accurint” report printouts in possession of a methamphetamine user heavily involved in identity theft. This agent’s aggressive follow-up investigation led to the

discovery of one of the most significant compromises of personal data in history. As of now, Lexis-Nexis, Accurint's parent company, has acknowledged the compromise of over 310,000 consumers' personal identifying information. Eighty-six existing customer accounts had their user names and passwords compromised, 57 unauthorized new accounts were created, and thousands of searches were run with reports generated. A joint investigation by local and federal agents assigned to REACT (including the FBI and Secret Service) has resulted in over 50 search warrants and subpoenas being served on suspects, ISPs, and electronic mail providers. Over a dozen computers have been seized and are undergoing examination. Five suspects are in custody or facing charges, and as many as 40 additional potential suspects with access to the compromised accounts have been identified.

$2 Million Platinum ID Fraud Cases

REACT participated with the FBI in tracking and apprehending four individuals engaged in corporate identity theft. The individuals posed as executives from Applied Materials, a local high tech company, and ordered $2.3 million in electronics-grade platinum via e-mail from a precious metals dealer. Agents substituted the platinum with stainless steel plates and inserted a hidden tracking device into containers. The agents tracked the shipment from the Bay Area to Los Angeles, through multiple changes in couriers and vehicles. The agents systematically tracked and arrested each courier after the cargo had changed hands. A federal grand jury indicted four suspects in a seven-count indictment.

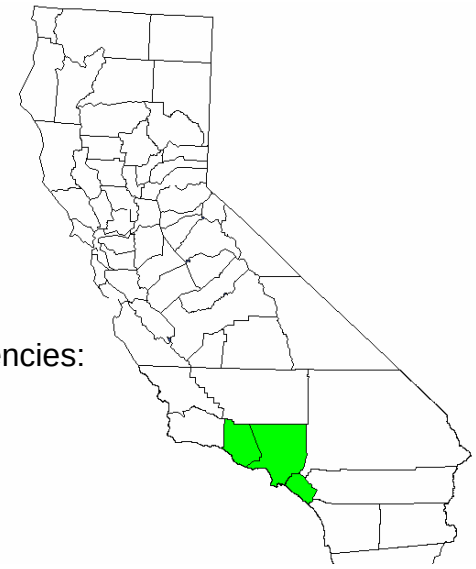
REACT Executive Committee/Steering Committee

REACT receives direction and oversight from a local Executive Committee and Steering Committee comprised of representatives from the local high technology and financial industries, and representatives from allied agencies associated with REACT. The committees meet, at a minimum, quarterly. The following agencies are represented on the REACT Executive Committee and Steering Committee:

- Adobe Systems
- California Attorney General
- California Highway Patrol
- Cisco Systems
- Comcast
- eBay
- Federal Bureau of Investigation
- Fremont Police Department
- Hayward Police Department
- Intel
- Internal Revenue Service
- Menlo Park Police Department

- Mountain View Police Department
- Palo Alto Police Department
- Recording Industry Association of America
- San Francisco District Attorney
- San Francisco Police Department
- San Jose Police Department
- San Mateo Sheriff's Department
- Santa Clara County District Attorney
- Santa Clara County Sheriff's Department
- Santa Clara Police Department
- Santa Cruz Sheriff's Department
- South San Francisco Police Department
- Sun Microsystems
- U.S. Attorney's Office
- U.S. Customs Service
- U.S. Department of Homeland Security

Southern California High Tech Task Force (SCHTTF)
Lead Agency: Los Angeles Sheriff's Department



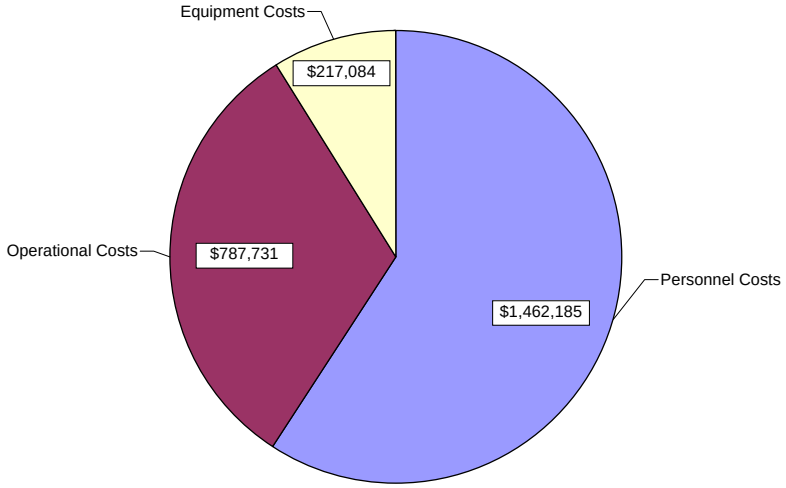
SCHTTF is represented by the following three counties:

- Los Angeles
- Orange
- Ventura

Through a memorandum of understanding,
SCHTTF is comprised of participants from the following agencies:

- Anaheim Police Department
- California Department of Justice
- California Highway Patrol
- Department of Motor Vehicles
- Federal Bureau of Investigations
- Internal Revenue Service
- Los Angeles City Attorney
- Los Angeles County District Attorney
- Los Angeles County Sheriff
- Los Angeles Police Department
- Office of Consumer Affairs
- Orange County District Attorney
- Orange County Sheriff
- Oxnard Police Department
- Pasadena Police Department
- Simi Valley Police Department
- Social Security
- U.S. Attorney
- U.S. Customs Service
- U.S. Postal Service
- U.S. Secret Service
- UCLA Police Department
- Ventura County District Attorney
- Ventura County Sheriff
- Ventura Police Department

SCHTTF – High Technology Crimes



During fiscal year 2004-05, SCHTTF received $1,973,600 in furtherance of the investigation of high technology crimes. SCHTTF provided a 25 percent match of these funds ($493,400) for a total grant award of $2,467,000. A breakdown of the budget categories is represented in the chart at the left.

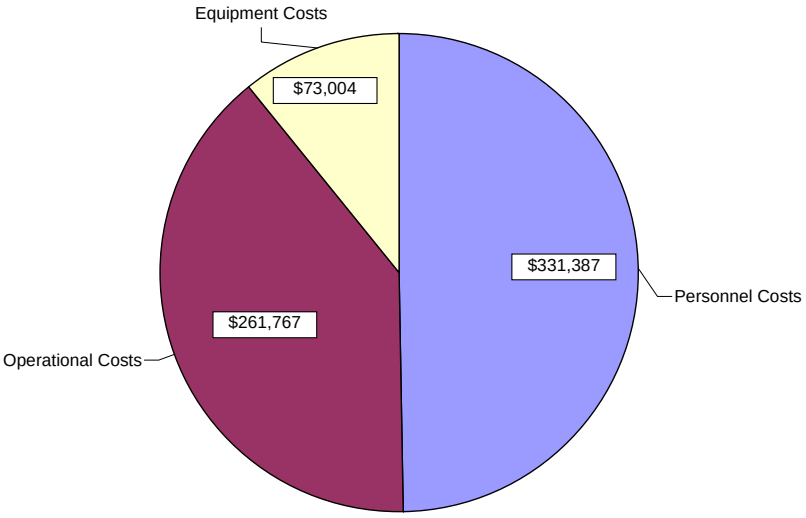
During the grant period, SCHTTF expended 59 percent of its high technology grant budget on personnel costs, 32 percent on operational costs, and 9 percent on equipment costs.

During the grant reporting period, SCHTTF

- Filed 92 cases involving high technology crimes
- Investigated 162 cases involving high technology crimes
- 3,209 victims were involved in the cases filed
- 75 convictions were obtained
- $56,922,722 in total aggregate monetary loss was suffered by the victims.

SCHTTF – Identity Theft Crimes

During fiscal year 2004-05, SCHTTF received $653,500 in furtherance of the investigation of identity theft crimes. SCHTTF provided a 25 percent match of these funds ($163,375) for a total grant award of $816,875. A breakdown of the budget categories is represented in the chart to the right.



During the grant period, SCHTTF expended 50 percent of its identity theft grant budget on personnel costs, 39 percent on operational costs, and 11 percent on equipment costs.

During the grant reporting period, SCHTTF

- Filed 119 cases involving identity theft crimes
- Investigated 917 cases involving identity theft crimes
- 2,492 victims were involved in the cases filed
- 95 convictions were obtained
- $2,396,612 in total aggregate monetary loss was suffered by the victims.

SCHTTF Identity Theft Case Highlights

A data aggregator company was compromised. The investigation is ongoing, and the investigative efforts have been joined with other federal agencies. The impact of the case has reached a national concern among the public and privacy rights groups.

SCHTTF Steering Committee

SCHTTF receives direction and oversight from a local Steering Committee comprised of representatives from the local high technology and financial industries, and representatives from allied agencies associated with SCHTTF. The following agencies are represented on the SCHTTF Steering Committee:

- California State Automobile Association (AAA)
- Adelphia Communications
- American Express
- AOL Time Warner
- AT&T Wireless Service
- Brotby & Associates
- Buy.Co
- Cellnet, LLC
- Earthlink
- Executive Software
- Exodus
- Falcon
- Greenwood & Associates
- IBM Corporation
- MACE Group
- MCI Worldcom
- Microsoft
- Motion Picture Association of America
- Nextel
- NICB
- NLECTC

- Pacific Bell
- Pacific Telesis Group
- Recording Industry Association of America
- Software Council of California
- Sony Corporation
- Sprint PCS
- Telegent
- TelePacific Communications
- Verizon Wireless
- VISA USA
- X.Com/Pay Pal, Inc.

Computer and Technology Crime High-Tech Response Team (CATCH)
Lead Agency: San Diego District Attorney's Office

CATCH is represented by the following three counties:

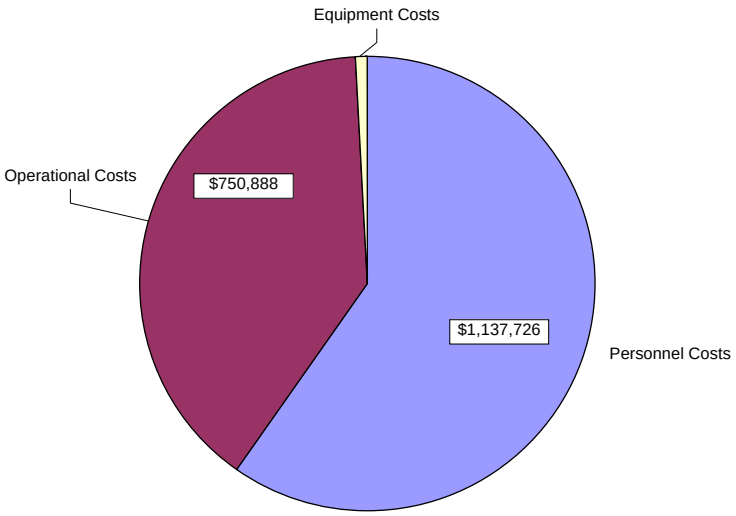
- Imperial
- Riverside
- San Diego

Through a memorandum of understanding, CATCH is comprised of participants from the following agencies:

- Bureau of Immigration and Customs Enforcement
- California Attorney General
- California Department of Justice
- California State Parole
- Carlsbad Police Department
- Department of Motor Vehicles
- Federal Bureau of Investigation
- Imperial County District Attorney's Office
- Internal Revenue Service
- Riverside County District Attorney's Office
- Riverside County Probation Department
- Riverside County Sheriff's Department
- San Diego County District Attorney
- San Diego County Probation
- San Diego County Sheriff
- San Diego Police Department
- U.S. Postal Inspector
- U.S. Secret Service

CATCH – High Technology Crimes

During Fiscal Year 2004-05, CATCH received $1,973,600 in furtherance of the investigation of high technology crimes. CATCH provided a 25 percent match of these funds ($493,400) for a total grant award of $2,467,000. A breakdown of the budget categories is represented in the chart on the following page.



During the grant period, CATCH expended 60 percent of its high technology grant budget on personnel costs, 39 percent on operational costs, and 1 percent on equipment costs.

During the grant reporting period, CATCH

- Filed 38 cases involving high technology crimes
- Investigated 155 cases involving high technology crimes
- 274 victims were involved in the cases filed
- 30 convictions were obtained
- $1,497,465 in total aggregate monetary loss was suffered by the victims

CATCH High Technology Case Highlights

Examples of cases investigated include:

05AS056R: A County Schools Superintendent reported receiving annoying phone calls and embarrassing emails sent to the County Office of Education faculty and board members. An investigation has led to several search warrants and tracing cyber trails to a public location with log-ins on several computers. The suspect is still being tracked.

05CC3083R: A suspect, working with accomplices, withdrew over $300,000 from a major business' payroll account through a large banking institution. The business runs tens of millions of dollars through the account each month. The suspects deposited the stolen funds into an E*Trade account and funneled some of those funds into a personal credit card account. Some suspects have been identified and search warrants have yielded documents, computers, and other evidence. The structure in which the evidence was found may be pursued for forfeiture.

05AS0064R: A law enforcement agency's digitally-recorded interviews in a homicide case were accidentally deleted. CATCH, pursuant to request, is attempting to recover the deleted recordings.

05FR0051R: CATCH is assisting the investigation of a murder/suicide via search of three computers, video and digital cameras, pagers and cell phones for any information related to the case.

05FR0045R: Assisted in the investigation of a robbery/murder in one county and a second murder in an adjoining county. This included a search of cell phones to gather stored images, telephone numbers, names, addresses and telephone records, text messages, e-mails, appointment records, digital memos, incoming and outgoing call records.

05FR0042R: Assist the bomb squad in examining memory devices and a laptop hard drive for information or files related to explosives, bombs, military ordinance, grenades, booby traps and other improvised explosive device information.

05FR0048R: Search a hard drive for bank routing or checking numbers, credit card numbers or accounts in different names, personal profiles, check writing programs, text messages to specific names, internet purchases, two home address, business names and other identity theft or check fraud materials.

05FR0040R: Assist law enforcement (homicide division). Download photos of subject holding/displaying weapon and any individual photos of same subject and/or weapon in any other photos. Also search for any phone numbers, text messages to or from noted person.

05FR0039R: Forensically examine video recording equipment from a private business that may have captured a shooting/murder that occurred on a nearby roadway.

05FR0037R: Assist a law enforcement Special Investigation Bureau request to search hard drives for marijuana-related information on a multi-site marijuana farm.

05FR0033R: Forensic examination of evidence recovered where suspects were financing narcotics sales through identity theft and fraud schemes.

05FR0032R: Examine victim's computer to search for on-line friends (buddy lists, chat, e-mail, etc.) and motive for a murder.

05CC3066R: Suspect lists auction items and fails to deliver items. Investigate and follow cyber trail leads to track suspect and recover evidence.

ABO061: Defendant sent email attachments of child pornography. His AOL account was terminated. He again opened another AOL account and sent child pornography again. His account was again terminated. A search warrant on his residence found him in possession of numerous images of child pornography. Forensics on his seized computer shows three other instances in which he sent child pornography.

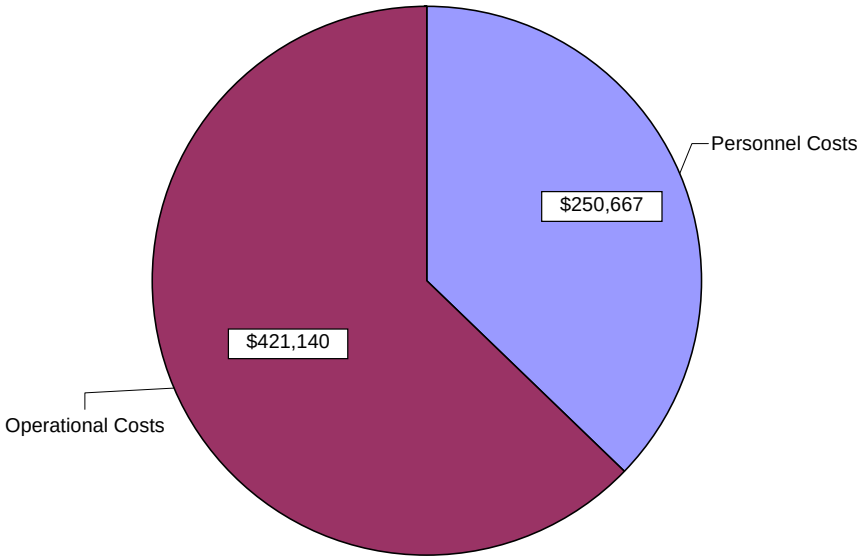
ABN288: Defendants purchase major league baseball tickets over internet via stolen credit card numbers. Tickets are delivered via e-mail and printed by home printer. Defendants advertised the tickets for sale in newspaper and on internet and sold them

to unsuspecting victims who discover that the tickets are not valid when they get to the gate at the game. CATCH gets tip and set up a sting. After the buy the defendants are arrested and their car searched. Computer, scanner and printer are recovered along with drugs and other evidence.

ABE520: Defendant sold counterfeit software through ads in newspapers and in two different undercover buys to CATCH investigator. The software was analyzed by Microsoft laboratory and determined to be counterfeit. Case was previously charged by the U.S. Attorney's Office, but dismissed against this defendant. There are a number of others charged and convicted in this scam on the federal side. The remaining defendant was convicted in state court.

CATCH – Identity Theft Crimes

During the Fiscal Year 2004-05, CATCH received $653,500 in furtherance of the investigation of identity theft crimes. CATCH provided a 25 percent match of these funds ($163,375) for a total grant award of $816,875. A breakdown of the budget categories is represented in the chart to the right.



During the grant period, CATCH expended 37 percent of its identity theft grant budget on personnel costs, 63 percent on operational costs, and none on equipment costs.

During the grant reporting period, CATCH

- Filed 213 cases involving identity theft crimes
- Investigated 292 cases involving identity theft crimes
- 801 victims were involved in the cases filed
- 139 convictions were obtained
- $1,887,872 in total aggregate monetary loss was suffered by the victims

CATCH Identity Theft Case Highlights

Examples of cases investigated include:

ABL355: A handful of individuals (one main character) engaged nearly one hundred people in a scheme involving several distinct groups: mail thieves, check washers, check forgers, solicitors of personal identifying information and access cards, bank account access providers, bogus check depositors and money withdrawers. The solicitors sought out young people in need of money and convinced them to turn over identification cards (e.g., a driver license), bank account number and PIN, and other personal identifying information in exchange for the promise of $500 to $3000 within a couple of weeks. Mail thieves provided stolen checks en route to pay bills. Check washers converted the stolen checks to "clean" checks. Forgers then re-wrote the checks payable to the providers of the personal identifying information, in amounts roughly between $5,000-$9,000. Depositors then deposited $30,000 to $80,000 in a single account over period of about two days. The main suspect then waited approximately 48 hours when the normal hold on the deposited checks was lifted but the checks had not yet cleared the payor bank. The main suspect checked via telephone using the automated information system of the bank and the PIN of the account holder to ascertain that the money (created by fraudulent checks) was available for withdrawal. The withdrawers then emptied the account systematically accessing numerous different branches and brought the loot to the main suspect. The scheme was carried out for years. CATCH and the United States Postal Inspection Service (which is a member agency with CATCH) conducted a lengthy investigation and developed informants. After months of executing search warrants, reviewing bank records, and interviewing witnesses and suspects, a CATCH prosecutor selected about 35 of potentially 100 defendants to initially charge with crimes. The prosecutor presented the case to the grand jury, which returned an indictment against the 35 defendants. Extraordinary coordination among scores of federal, state and local officers led to a day of warrant service and arrests of the defendants – some were out of the state and some out of the country. All were apprehended. Their trials are currently pending.

ABN133: The suspects had pending cases, but were continuing to acquire stolen identities and go on shopping sprees. CATCH received several complaints from victim businesses and began to work the case. While in the field, CATCH investigators were contacted by a home goods store indicating that the suspects were in the store buying things with stolen access cards. A CATCH ID Team went to the store and apprehended the suspects as they entered their vehicle. Good police work led to the discovery of the apartment where the suspects were living and a search pursuant to a probation waiver was conducted. The entire contents of the apartment and attached garage were acquired with stolen access cards. Other law enforcement agencies assisted with moving vans as the entire contents were seized (furniture, clothing, bedding, motor vehicles, firearms, computer equipment, other electronics, plants, dishes, utensils, sophisticated surveillance system, etc.) Victim stores were notified for identification and return, or other disposition. Found in the apartment was a copy of a previous search

warrant served on the defendants months earlier as a result of the same type of activity. The defendants await trial.

ABM808: A re-labeling of boxes of computer equipment at the warehouse of an international shipping company, to be rerouted to the home address of a company employee or his associates. Payment for the rerouted shipping was assessed to a major client's account so that the charges blended in with the thousands of dollars in shipping each month.

CATCH Steering Committee

CATCH receives direction and oversight from a local Steering Committee comprised of representatives from the local high technology industry, financial industry, and representatives from allied agencies associated with CATCH. The Steering Committee meets, at a minimum, quarterly. The following agencies are represented on the CATCH Steering Committee:

- AeA
- Border Research & Technology Center
- California Attorney General
- California Department of Motor Vehicles
- California Department of Justice
- California State Parole
- CafeSoft
- Carlsbad Police Department
- San Diego City Attorney's Office
- Computer Conversion
- Cox Communications
- Evident Data, Inc.
- Federal Bureau of Investigations
- High Technology Crime Investigation Association
- ICE
- Imperial County
- Internal Revenue Service
- Linksys
- MedImpact Healthcare System, Inc.
- Open Doors Software
- Peterbuilt
- Practical Security
- Qualcomm

- Ranger Online Corporation
- RCFL Forensic Lab
- Riverside Adult Probation
- Riverside County Sheriff
- Riverside County Probation
- SAIC
- SBC
- San Diego Sheriff
- San Diego County Probation
- San Diego District Attorney
- San Diego Police Department
- SDRIW
- Software Design Assoc.
- Sony
- Sony Computer Entertainment
- Source 4, Inc.
- SPAWAR
- Time Warner Cable
- Time Warner ISP
- U.S. Encode Corporation
- U.S. Department of Justice
- U.S. Postal Inspection
- U.S. Secret Service
- Volonet/Redwire ISP
- Voyager Systems, Inc.
- Websense

APPENDIX A

California Penal Code Sections 13848-13848.8.

13848. (a) It is the intent of the Legislature in enacting this chapter to provide local law enforcement and district attorneys with the tools necessary to successfully interdict the promulgation of high technology crime. According to the federal Law Enforcement Training Center, it is expected that states will see a tremendous growth in high technology crimes over the next few years as computers become more available and computer users more skilled in utilizing technology to commit these faceless crimes. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which is the target of a criminal act.

(b) Funds provided under this program are intended to ensure that law enforcement is equipped with the necessary personnel and equipment to successfully combat high technology crime which includes, but is not limited to, the following offenses:

(1) White-collar crime, such as check, automated teller machine, and credit card fraud, committed by means of electronic or computer-related media.

(2) Unlawful access, destruction of or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wireline communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, or unauthorized disclosure of data stored within those computers and networks.

(3) Money laundering accomplished with the aid of computer networks or electronic banking transfers.

(4) Theft and resale of telephone calling codes, theft of telecommunications service, theft of wireless communication service, and theft of cable television services by manipulation of the equipment used to receive those services.

(5) Software piracy and other unlawful duplication of information.

(6) Theft and resale of computer components and other high technology products produced by the high technology industry.

(7) Remarking and counterfeiting of computer hardware and software.

(8) Theft of trade secrets.

(c) This program is also intended to provide support to law enforcement agencies by providing technical assistance to those agencies with respect to the seizure and analysis of computer systems used to commit high technology crimes or store evidence relating to those crimes.

13848.2. (a) There is hereby established in the agency or agencies designated by the Director of Finance pursuant to Section 13820 a program of financial and technical assistance for law enforcement and district attorneys' offices, designated the High Technology Theft Apprehension and Prosecution Program. All funds appropriated to the agency or agencies designated by the Director of Finance pursuant to Section 13820 for the purposes of this chapter shall be administered and disbursed by the executive director of the office in consultation with the High Technology Crime Advisory Committee as established in Section 13848.6 and shall to the extent feasible be coordinated with federal funds and private grants or private donations that are made available for these purposes.

(b) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 is authorized to allocate and award funds to regional high technology crime programs which are established in compliance with Section 13848.4.

(c) The allocation and award of funds under this chapter shall be made on application executed by the district attorney, county sheriff, or chief of police and approved by the board of supervisors for each county that is a participant of a high technology theft apprehension and prosecution unit.

(d) In identifying program areas that will be eligible for competitive application during the 1998-99 fiscal year for federal funding pursuant to the Edward Byrne Memorial State and Local Law Enforcement Assistance Programs (Subchapter V (commencing with Section 3750) of Chapter 46 of the United States Code), the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall include, to the extent possible, an emphasis on high technology crime by selecting funding areas that would further the use of federal funds to address high technology crime and facilitate the establishment of high technology multijurisdictional task forces.

(e) The agency or agencies designated by the Director of Finance pursuant to Section 13820 shall allocate any increase in federal funding pursuant to the Anti-Drug Abuse Act (Public Law 100-690) for the 1998-99 fiscal year to those programs described in subdivision (d).

13848.4. (a) All funds appropriated to the agency or agencies designated by the Director of Finance pursuant to Section 13820 for the purposes of this chapter shall be deposited in the High Technology Theft Apprehension and Prosecution Program Trust Fund, which is hereby established. The fund shall be under the direction and control of the executive director. Moneys in the fund, upon appropriation by the Legislature, shall be expended to implement this chapter.

(b) Moneys in the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement and prosecutors to deter, investigate, and prosecute high technology related crimes. After deduction of the actual and necessary administrative costs referred to in subdivision (f), the High Technology Theft Apprehension and Prosecution Program Trust Fund shall be expended to fund programs to enhance the capacity of local law enforcement, state police, and local prosecutors to deter, investigate, and prosecute high technology related crimes. Any funds distributed under this chapter shall be expended for the exclusive purpose of deterring, investigating, and prosecuting high technology related crimes.

(c) Up to 10 percent of the funds shall be used for developing and maintaining a statewide database on high technology crime for use in developing and distributing intelligence information to participating law enforcement agencies. In addition, the Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 may allocate and award up to 5 percent of the funds available to public agencies or private nonprofit organizations for the purposes of establishing statewide programs of education, training, and research for public prosecutors, investigators, and law enforcement officers relating to deterring, investigating, and prosecuting high technology related crimes. Any funds not expended in a fiscal year for these purposes shall be distributed to regional high technology theft task forces pursuant to subdivision (b).

(d) Any regional task force receiving funds under this section may elect to have the Department of Justice administer the regional task force program. The department may be reimbursed for any expenditures incurred for administering a regional task force from funds given to local law enforcement pursuant to subdivision (b).

(e) The agency or agencies designated by the Director of Finance pursuant to Section 13820 shall distribute funds in the High Technology Theft Apprehension and Prosecution Program Trust Fund to eligible agencies pursuant to subdivision (b) in consultation with the High Technology Crime Advisory Committee established pursuant to Section 13848.6.

(f) Administration of the overall program and the evaluation and monitoring of all grants made pursuant to this chapter shall be performed by the agency or agencies designated by the Director of Finance pursuant to Section 13820, provided that funds expended for these functions shall not exceed 5 percent of the total amount made available under this chapter.

13848.6. (a) The High Technology Crime Advisory Committee is hereby established for the purpose of formulating a comprehensive written strategy for addressing high technology crime throughout the state, with the exception of crimes that occur on state property or are committed against state employees, and to advise the agency or agencies designated by the Director of Finance pursuant to Section 13820 on the appropriate disbursement of funds to regional task forces.

(b) This strategy shall be designed to be implemented through regional task forces. In formulating that strategy, the committee shall identify various priorities for law enforcement attention, including the following goals:

(1) To apprehend and prosecute criminal organizations, networks, and groups of individuals engaged in the following activities:

(A) Theft of computer components and other high technology products.

(B) Violations of Penal Code Sections 211, 350, 351a, 459, 496, 537e, 593d, and 593e.

(C) Theft of telecommunications services and other violations of Penal Code Sections 502.7 and 502.8.

(D) Counterfeiting of negotiable instruments and other valuable items through the use of computer technology.

(E) Creation and distribution of counterfeit software and other digital information, including the use of counterfeit trademarks to misrepresent the origin of that software or digital information.

(2) To apprehend and prosecute individuals and groups engaged in the unlawful access, destruction, or unauthorized entry into and use of private, corporate, or government computers and networks, including wireless and wire line communications networks and law enforcement dispatch systems, and the theft, interception, manipulation, destruction, and unauthorized disclosure of data stored within those computers.

(3) To apprehend and prosecute individuals and groups engaged in the theft of trade secrets.

(4) To investigate and prosecute high technology crime cases requiring coordination and cooperation between regional task forces and local, state, federal, and international law enforcement agencies.

(c) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall appoint the following members to the committee:

(1) A designee of the California District Attorneys Association.

(2) A designee of the California State Sheriffs Association.

(3) A designee of the California Police Chiefs Association.

(4) A designee of the Attorney General.

(5) A designee of the California Highway Patrol.

(6) A designee of the High Technology Crime Investigation Association.

(7) A designee of the agency or agencies designated by the Director of Finance pursuant to Section 13820.

(8) A designee of the American Electronic Association to represent California computer system manufacturers.

(9) A designee of the American Electronic Association to represent California computer software producers.

(10) A designee of the California Cellular Carriers Association.

(11) A representative of the California Internet industry.

(12) A designee of the Semiconductor Equipment and Materials International.

(13) A designee of the California Cable Television Association.

(14) A designee of the Motion Picture Association of America.

(15) A designee of either the California Telephone Association or the California Association of Competitive Telecommunication Companies. This position shall rotate every other year between designees of the two associations.

(16) A representative of the California banking industry.

(17) A representative of the Office of Privacy Protection.

(18) A representative of the Department of Finance.

(d) The Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall designate the Chair of the High Technology Crime Advisory Committee from the appointed members.

(e) The advisory committee shall not be required to meet more than 12 times per year. The advisory committee may create subcommittees of its own membership,

and each subcommittee shall meet as often as the subcommittee members find necessary. It is the intent of the Legislature that all advisory committee members shall actively participate in all advisory committee deliberations required by this chapter.

Any member who, without advance notice to the executive director and without designating an alternative representative, misses three scheduled meetings in any calendar year for any reason other than severe temporary illness or injury (as determined by the Executive Director of the agency or agencies designated by the Director of Finance pursuant to Section 13820) shall automatically be removed from the advisory committee. If a member wishes to send an alternative representative in his or her place, advance written notification of this substitution shall be presented to the executive director. This notification shall be required for each meeting the appointed member elects not to attend.

Members of the advisory committee shall receive no compensation for their services, but shall be reimbursed for travel and per diem expenses incurred as a result of attending meetings sponsored by the agency or agencies designated by the Director of Finance pursuant to Section 13820 under this chapter.

(f) The executive director, in consultation with the High Technology Crime Advisory Committee, shall develop specific guidelines and administrative procedures for the selection of projects to be funded by the High Technology Theft Apprehension and Prosecution Program, which guidelines shall include the following selection criteria:

(1) Each regional task force that seeks funds shall submit a written application to the committee setting forth in detail the proposed use of the funds.

(2) In order to qualify for the receipt of funds, each proposed regional task force submitting an application shall provide written evidence that the agency meets either of the following conditions:

(A) The regional task force devoted to the investigation and prosecution of high technology-related crimes is comprised of local law enforcement and prosecutors, and has been in existence for at least one year prior to the application date.

(B) At least one member of the task force has at least three years of experience in investigating or prosecuting cases of suspected high technology crime.

(3) Each regional task force shall be identified by a name that is appropriate to the area that it serves. In order to qualify for funds, a regional task force shall be comprised of local law enforcement and prosecutors from at least two counties. At the time of funding, the proposed task force shall also have at least one investigator assigned

to it from a state law enforcement agency. Each task force shall be directed by a local steering committee composed of representatives of participating agencies and members of the local high technology industry.

(4) The California High Technology Crimes Task Force shall be comprised of each regional task force developed pursuant to this subdivision.

(5) Additional criteria that shall be considered by the advisory committee in awarding grant funds shall include, but not be limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, or corporations, as a result of the high technology crime cases filed, and those under active investigation by that task force.

(6) Each regional task force that has been awarded funds authorized under the High Technology Theft Apprehension and Prosecution Program during the previous grant-funding cycle, upon reapplication for funds to the committee in each successive year, shall be required to submit a detailed accounting of funds received and expended in the prior year in addition to any information required by this section. The accounting shall include all of the following information:

(A) The amount of funds received and expended.

(B) The use to which those funds were put, including payment of salaries and expenses, purchase of equipment and supplies, and other expenditures by type.

(C) The number of filed complaints, investigations, arrests, and convictions that resulted from the expenditure of the funds.

(g) The committee shall annually review the effectiveness of the California High Technology Crimes Task Force in deterring, investigating, and prosecuting high

technology crimes and provide its findings in a report to the Legislature and the Governor. This report shall be based on information provided by the regional task forces in an annual report to the committee which shall detail the following:

(1) Facts based upon, but not limited to, the following:

(A) The number of high technology crime cases filed in the prior year.

(B) The number of high technology crime cases investigated in the prior year.

(C) The number of victims involved in the cases filed.

(D) The number of convictions obtained in the prior year.

(E) The total aggregate monetary loss suffered by the victims, including individuals, associations, institutions, corporations, and other relevant public entities, according to the number of cases filed, investigations, prosecutions, and convictions obtained.

(2) An accounting of funds received and expended in the prior year, which shall include all of the following:

(A) The amount of funds received and expended.

(B) The uses to which those funds were put, including payment of salaries and expenses, purchase of supplies, and other expenditures of funds.

(C) Any other relevant information requested.

13848.8. (a) The executive director of the agency or agencies designated by the Director of Finance pursuant to Section 13820 shall also appoint the following members to the High Technology Crime Advisory Committee established by Section 13848.6:

(1) A designee of the Recording Association of America.

(2) A designee of the Consumers Union.

(b) The High Technology Crime Advisory Committee, in formulating a comprehensive written strategy for addressing high technology crime throughout the state, shall identify, in addition to the various priorities for law enforcement attention specified in subdivision (b) of Section 13848.6, the goal of apprehending and

prosecuting criminal organizations, networks, and groups of individuals engaged in the following activities:

(1) Violations of Sections 653h, 653s, and 635w.

(2) The creation and distribution of pirated sound recordings or audiovisual works or the failure to disclose the origin of a recording or audiovisual work.

APPENDIX B

Roster – High Technology Crime Advisory Committee

MEMBER/ADDRESS	DESIGNATION
James Sibley Deputy District Attorney – Santa Clara County 70 West Hedding Street, 4th Floor San Jose, CA 95110 (408) 792-2823 – phone (408) 792-8742 – fax jsibley@da.sccgov.org	California District Attorneys' Association *(Designation letter rec'd July 28, 2003)*
Chief Scott Vermeer Mountain View Police Department 1000 Villa Street Mountain View, CA 94041 (650) 903-6350 – phone (650) 903-6122 – fax scott.Vermeer@ci.mtnview.ca.us	California Police Chiefs' Association *(Designation letter rec'd June 18, 2003.)* Secretary: Mary Ann Helfrich (650) 903-6700
Rick Oules Director, Division of Law Enforcement Department of Justice 4949 Broadway Sacramento, CA 95820 (916) 227-3764 – phone	California Attorney General's Office Secretary: Donna Jenkins (916) 227-3884 Donna.Jenkins@doj.ca.gov
Asst. Chief Sal Segura California Highway Patrol 2555 1st Avenue, Room 200 Sacramento, CA 95818 (916) 657-7171 – phone (916) 657-8196 – fax ssegura@chp.ca.gov	California Highway Patrol *(Designation letter rec'd December 15, 2004)*

Lt. John McMullen
District Attorney-County of Santa Clara
Bureau of Investigation
High Technology Crime Unit
70 West Hedding Street, West Wing
San Jose, CA 95110
(408) 792-2879 - phone

jmcmullen@da.sccgov.org

High Tech Crime Investigation Association

(Designation letter rec'd May 31, 2005)

William E. Eyres, Vice Chair
8831 Berta Ridge Court
Prunedale, CA 93907
(831) 663-3695 – phone

eyres@montereybay.com

American Electronic Association
California Computer System Manufacturers

Robert Bastida
Director of Corporate Security – Oracle, Inc.

500 Oracle Parkway – M/S 6op1
Redwood City, CA 95065
(650) 506-5789 – phone
(650) 633-0531 - fax

robert.bastida@oracle.com

American Electronic Association
California Computer Software Producers

Paul S. Sieracki
Staff Director – Sprint (Wireless Carriers of CA)

Sprint – Law & External Affairs
925 L Street, Suit 345
Sacramento, CA 95814
(916) 441-0973 – phone
(916) 441-0945 – fax

paul.s.sieracki@mail.sprint.com

California Cellular Carriers Association

(Designation letter rec'd March 23, 2005)

Robert Chestnut
Vice President, Rules, Trust & Safety
eBay, Inc.
2145 Hamilton Avenue
San Jose, CA 95125
(408) 376-5945 – phone

robc@ebay.com

California Internet Industry

(Designation letter rec'd Sept. 4, 2003)

Saul Arnold
Etec Systems, Inc.
26460 Corporate Avenue
Hayward, CA 94545
(510) 887-3550 – phone

sarnold@etec.com

Semiconductor Equipment and Materials International

(Designation letter rec'd December 7, 1998)

Bill Bowyer
Comcast Cable
501 Guiseppe Court, Suite D
Roseville, CA 95678
(916) 218-3852 – phone
(916) 786-9535 - fax

bill_bowyer@cable.comcast.com

California Cable & Telecommunications Association

(Designation letter rec'd Sept. 5, 2003)

Chuck Hausman
Deputy Director
Motion Picture Association of America, Inc
15503 Ventura Boulevard
Encino, CA 91436
(818) 995-6600 – phone
(818) 382-1785 – fax

chuck_hausman@mpaa.com

Motion Picture Association of America

(Designation letter rec'd Sept. 17, 2004)

Secretary, Heather Flores
(818) 995-6600

Mark Yamane
2600 Camino Ramon, Room 1CS95
San Ramon, CA 94583
(925) 543-8030 – phone
(925) 866-2717 – fax

my1259@sbc.com

California Telephone Association/California Association of Long Distance Companies

(Designation letter rec'd April 20, 2001)

Secretary: Esther Monetti
(925) 543-8002

Lieutenant Adam Christianson
Administrative Services Division
250 East Hackett Road
Modesto, CA 95358

chradam@stanislaussheriff.com

California State Sheriffs' Association

(Designation letter rec'd December 28, 2004)

Gail Hillebrand
Senior Attorney
1535 Mission Street
San Francisco, CA 94103
(415) 431-6747 – phone
(415) 431-0906 – fax

hillga@consumer.org

Representative of the Consumer's Union

Gary Reynolds
Director, Financial Crime Investigations
Wells Fargo Bank
420 Montgomery Street, 4th Floor
San Francisco, CA 95104
(415) 396-4032 – phone
(415) 788-6843 – fax

reynoldg@wellsfargo.com

Representative of the California Banking Industry

(Designation letter rec'd June 30, 2005)

Assistant: Lily Tam
(415) 396-2986
tamlily@wellsfargo.com

Charles A. Lawhorn
Anti-Piracy Legal Affairs
10842 Noel Street, Unit 106
Los Alamitos, CA 90720
(714) 236-0830 – phone
(714) 236-0930 – fax

clawhorn@riaa.com

Representative of the Recording Industry Association of America

(Designation letter rec'd Oct. 18, 2004)

Debra Reiger
State Information Security Officer
Office of Technology Review-Oversight & Security Unit
Department of Finance
915 L Street, 6th Floor
Sacramento, CA 95814
(916) 445-1777 - phone

Representative of the Department of Finance

(Designation letter rec'd May 31, 2005)

Joanne McNabb, Chief
Office of Privacy Protection
400 R Street, Suite 3080
Sacramento, CA 95814
(916) 322-4420 – phone
(916) 323-8451 - fax

Joanne_mcnabb@dca.ca.gov

Representative of the Office of Privacy Protection

(Designation rec'd Mar. 3. 2004)

Secretary: Angela Bigelow
(916) 322-1271
angela_bigelow@dca.ca.gov

Clark Kelso – Chair
State of California
Chief Information Officer
3455 Fifth Avenue
Sacramento, CA 95817
(916) 739-7302 – phone
(916) 739-7072 - fax

ckelso@pacific.edu

State of California

(Designation rec'd March 12, 2004)

Priscilla Dodson
(916) 739-7302
pdodson@pacific.edu

APPENDIX C
Roster – Regional Task Forces – High Tech

Northern California Computer Crimes Task Force (NC^{3}TF)
Mr. Edward Berberian – Project Director; Lt. Rick Nichelman – Project Manager
455 Devlin Road, Suite 207
Napa, CA 94558
Website: www.nc3tf.org
Phone: 707-253-4500
Fax: 707-253-4664

Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)
Capt. Wayne Ikeuchi – Project Director; Lt. Bob Lozito – Project Manager
4510 Orange Grove Avenue
Sacramento, CA 95841
Website: www.sachitechcops.org
Phone: 916-874-3002
Fax: 916-874-3006

Rapid Enforcement Allied Computer Team (REACT)
Mr. James Sibley – Project Director/Project Manager
950 South Bascom Avenue, Suite 3011
San Jose, CA 95128
Website: www.reacttf.org
Phone: 408-494-7186
Fax: 408-287-5076

Southern California High Tech Task Force (SCHTTF)
Lt. Robert Costa – Project Director; Sgt. Anthony Lucia – Project Manager
9900 Norwalk Boulevard, Suite 150
Santa Fe Springs, CA 90670
Phone: 562-347-2601
Fax: 562-946-7506

Computer and Technology Crime High-Tech Response Team (CATCH)
Mr. Keith Burt – Project Director; Lt. Terry Jensen – Project Manager
4725 Mercury Street, Suite 200
San Diego, CA 92111
Website: www.catchteam.org
Phone: 619-531-3660
Fax: 858-715-2366

APPENDIX D
Roster – Regional Task Forces – Identity Theft

Northern California Computer Crimes Task Force (NC^{3}TF)
Mr. Edward Berberian – Project Director; Lt. Rick Nichelman – Project Manager
455 Devlin Road, Suite 207
Napa, CA 94558
Website: www.nc3tf.org
Phone: 707-253-4500
Fax: 707-253-4664

Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)
Lt. Bob Lozito – Project Director; Sgt. Mike Freeworth – Project Manager
4510 Orange Grove Avenue
Sacramento, CA 95841
Website: www.sachitechcops.org
Phone: 916-874-3000
Fax: 916-874-3006

Rapid Enforcement Allied Computer Team (REACT)
Mr. James Sibley – Project Director/Project Manager
Sgt. Art Martinez – Identity Theft Supervisor
950 South Bascom Avenue, Suite 3011
San Jose, CA 95128
Website: www.reacttf.org
Phone: 408-994-7186; 650-599-7390
Fax: 408-287-5076

Southern California High Tech Task Force (SCHTTF)
Lt. Ronald Williams – Project Director; Sgt. Robert Berardi – Project Manager
9900 Norwalk Boulevard, Suite 150
Santa Fe Springs, CA 90670
Fax: 562-347-2660

Computer and Technology Crime High-Tech Response Team (CATCH)
Mr. Keith Burt – Project Director; Lt. Terry Jensen – Project Manager
Fr. Fred Baclagan – Identity Theft Supervisor
4725 Mercury Street, Suite 200
San Diego, CA 92111
Website: www.catchteam.org
Phone: 619-531-3660
Fax: 858-715-2366

APPENDIX E

STATE OF CALIFORNIA
BYLAWS, RULES AND PROCEDURES
OF THE
HIGH TECHNOLOGY CRIME ADVISORY COMMITTEE

Adopted: June 2005
Revised: March 2005

ARTICLE I: NAME AND AUTHORITY

This organization, created in the State government by statutory authority, shall be known as the High Technology Crime Advisory committee – hereinafter referred to as the "Committee."

ARTICLE II: MEMBERSHIP AND CHAIRPERSON SELECTION

Section 1.
The Committee shall be composed of twenty members. The Committee membership shall include:

(1) A designee of the California Attorney General;
(2) A designee of the California Highway Patrol
(3) A designee of the California Office of Emergency Services;
(4) A representative of the California Department of Finance;
(5) A representative of the California Office of Privacy Protection;
(6) A designee of the California District Attorneys Association;
(7) A designee of the California State Sheriff's Association;
(8) A designee of the California Police Chief's Association;
(9) A designee of the High Tech Criminal Investigators Association;
(10) A designee of the American Electronic Association to represent California computer system manufacturers;
(11) A designee of the American Electronic Association to represent California software producers;
(12) A designee of the California Cellular Carriers Association;
(13) A designee of the California Internet Industry;
(14) A designee of the Semiconductor Equipment and Materials International (SEMI);
(15) A designee of the California Cable Television Association;
(16) A designee of the Motion Picture Association of America
(17) A designee of either the California Telephone Association **or** the California Association of Competitive Telecommunications Companies (CALTEL). This position shall rotate every other year between designees of the two associations;
(18) A representative of the California Banking Industry;
(19) A designee of the Recording Industry Association of America
(20) A designee of the Consumers Union

ARTICLE II *(continued)*

Section 2.
The chairperson of the Committee shall be selected by the Executive Director of the Office of Emergency Services from among the members of the Committee [Penal Code Section 13848.6(d)].

ARTICLE III: POWERS AND DUTIES

Section 1.

The Committee is empowered to act as the advisory board of the Office of Emergency Services in accordance with the mandates of the pertinent state acts and programs. The Committee may develop and/or modify and recommend to the Office of Emergency Services a high technology plan.

Section 2.

The Committee may develop policy recommendations for the Governor, the Legislature, the Office of Emergency Services and the local units of government on major criminal justice issues where a high technology nexus exists. To that end, the Committee understands itself to be the primary advisory board on technology-related criminal justice issues. Its goals include:

1. Identifying current, developing and future issues involving high technology crime and criminal justice policy and procedures relevant to such issues;
2. Developing an understanding of the issues attendant to high technology crime and making conclusions that provide the foundation for recommendations to the Office of Emergency Services, the Governor and the Legislature concerning high technology crime, criminal identification, apprehension and prosecution;
3. Issuing analysis of current or pending high technology criminal justice-related legislation;
4. Assisting California's criminal justice agencies and practitioners in the effective use of resources regarding high technology crime;
5. Coordinating studies and recommendations with the Office of Emergency Services and other criminal justice agencies with a view toward isolating issues common to high technology crime and justice.

ARTICLE IV: COMMITTEE MEETINGS

Section 1.

The Committee shall meet at such intervals as necessary to carry out its duties, but no more than twelve meetings shall be held annually. Regular meetings of the Committee shall be held at least quarterly unless, in the opinion of the Committee Chair and Vice Chair, there are insufficient items of business or insufficient funds to call such quarterly or regular meetings. The Executive Secretary of the Committee shall give a minimum of ten days written advance notice to the membership of the Committee of the time and place of a regular meeting.

ARTICLE IV: *(continued)*

Section 2.

Special meetings of the Committee may be called at any time by the Committee Chair. Forty-eight hours prior notice of the time and place of such special meetings shall be given by the Chair to the members, where permitted by law.

Section 3.

Meetings shall be conducted in accordance with these bylaws and Robert's Rules of Order.

ARTICLE V: SUBCOMMITTEES AND SUBCOMMITTEE MEETINGS

Section 1.

The Committee shall have the following subcommittees:

--Strategy Subcommittee
--Bylaws Subcommittee

Section 2.

The Committee may recommend the creation of such subcommittees of its own membership as it deems necessary.

Section 3.

By a majority decision, the Committee may request the review of any subcommittee's decisions or activities.

Section 4.

Each subcommittee of the Committee shall meet as often as the subcommittee members find to be necessary.

Section 5.

All subcommittees shall be ad hoc in nature, and sit at the pleasure of the Committee Chair and a majority vote of the membership present at the time of the subcommittee creation.

ARTICLE VI: OFFICERS AND DUTIES

Section 1.

The officers of the Committee shall be the Chairperson (Chair) and the Vice Chairperson (Vice Chair).

Section 2.

The Chairperson shall be chosen by the Executive Director of the Office of Emergency Services from among members of the Committee, and shall serve at the pleasure of the Director. The Vice Chair shall be chosen by the membership of the Committee from among members of the Committee.

Section 3.

The Chair shall preside over all meetings of the Committee, and perform such additional duties as requested by the Committee and normally executed by a chairperson. The Chair shall create such standing and ad hoc committees as are deemed necessary to carry out the powers, duties

and mission of the Committee. The Chair also shall appoint all members to both standing and ad hoc committees. All such subcommittee members shall serve at the pleasure of the Chair.

Section 4.

In the absence of the Chair, the Vice Chair shall preside at meetings and perform such additional duties as are required by the Committee and necessitated by the absence of the Chair.

Section 5.

In the event a vacancy occurs in the office of the Chairperson, the Director shall designate a successor prior to the next regular or special meeting. In the event a vacancy occurs in the office of the Vice Chairperson, the membership of the Committee shall designate a successor at the next regular or special meeting (Penal Code 13810).

ARTICLE VII: QUORUM, VOTING AND ATTENDANCE

Section 1.

A quorum of the Committee for any meeting shall consist of a majority of the members designated or appointed at the time of the meeting. If a quorum is present, a majority vote of the members present is necessary for Committee action, except for the suspension of these bylaws pursuant to Article XII.

Section 2.

No vote by an alternate will be honored except as provided for in this section.

a) An alternate designation letter is required from any absent Committee member, and shall be presented to the Committee prior to the start of the next regular or special meeting.
b) An alternate will have full voting rights, floor rights, and be included in quorum determinations.
c) Alternated attendance for a Committee member will negate provision of Section 3 below.

Section 3.

Any member of the Committee who misses three consecutive meetings or who attends less than fifty percent of the Committee's regularly called meetings during one calendar year shall be automatically removed from the Committee, except in situations in which the Chair finds that such deficiency is the result of illness or injury.

ARTICLE VIII: REIMBURSEMENT OF EXPENSES

Section 1.

Members of the Committee shall not receive compensation for their services but will be reimbursed for those actual and necessary expenses incurred which relate to their duties as Committee members.

Section 2.

Members of continuing task forces, review committees or of any other Committee-established auxiliary bodies who are not Committee members shall not receive compensation for expenses, unless prior approval has been obtained from the Office of Emergency Services. However,

ARTICLE VIII *(continued)*

individuals who appear before the Committee at its request in order to review specific topics on one or more occasions shall be reimbursed for their necessary travel expenses.

ARTICLE IX: EXECUTIVE SECRETARY

Section 1.

The Executive Secretary of the Committee shall be appointed by the Director of the Office of Emergency Services

Section 2.

The duties of the Executive Secretary to the Committee shall be to provide staff support to the Committee including keeping all records, preparing agendas for each meeting, keeping minutes and approving all Committee expenditures.

Section 3.

The Executive Secretary shall, in accordance with applicable law, be responsible for any additional staffing, planning, organizing, coordinating, and directing to those activities necessary to assure the fulfillment of the powers, duties, and mission of the Committee.

ARTICLE X: CONFLICT OF INTEREST

Section 1.

No member of the Committee shall participate personally through decision, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise in any proceeding, application, request for a ruling or other determination, contract, grant claim controversy, or other particular matter in which funds under jurisdiction of the Committee are used, where to his or her knowledge he or she or his or her immediate family, partners, organization other than a public agency in which he or she is serving is an officer, director, trustee, partner, or employee or any person or organization with who he or she is negotiating or has any arrangement concerning prospective employment, has a financial interest.

Section 2.

In the review of proposals under appeal before the Committee, members of the Committee shall avoid any action which might result in, or create the appearance of:

a) Using his or her official position for private gain;
b) Giving preferential treatment to any person;
c) Losing complete independence or impartiality;
d) Making an official decision outside official channels; or
e) Affecting adversely the confidence of the public in the integrity of the Government or the program.

ARTICLE XI: AMENDMENTS TO THE BYLAWS

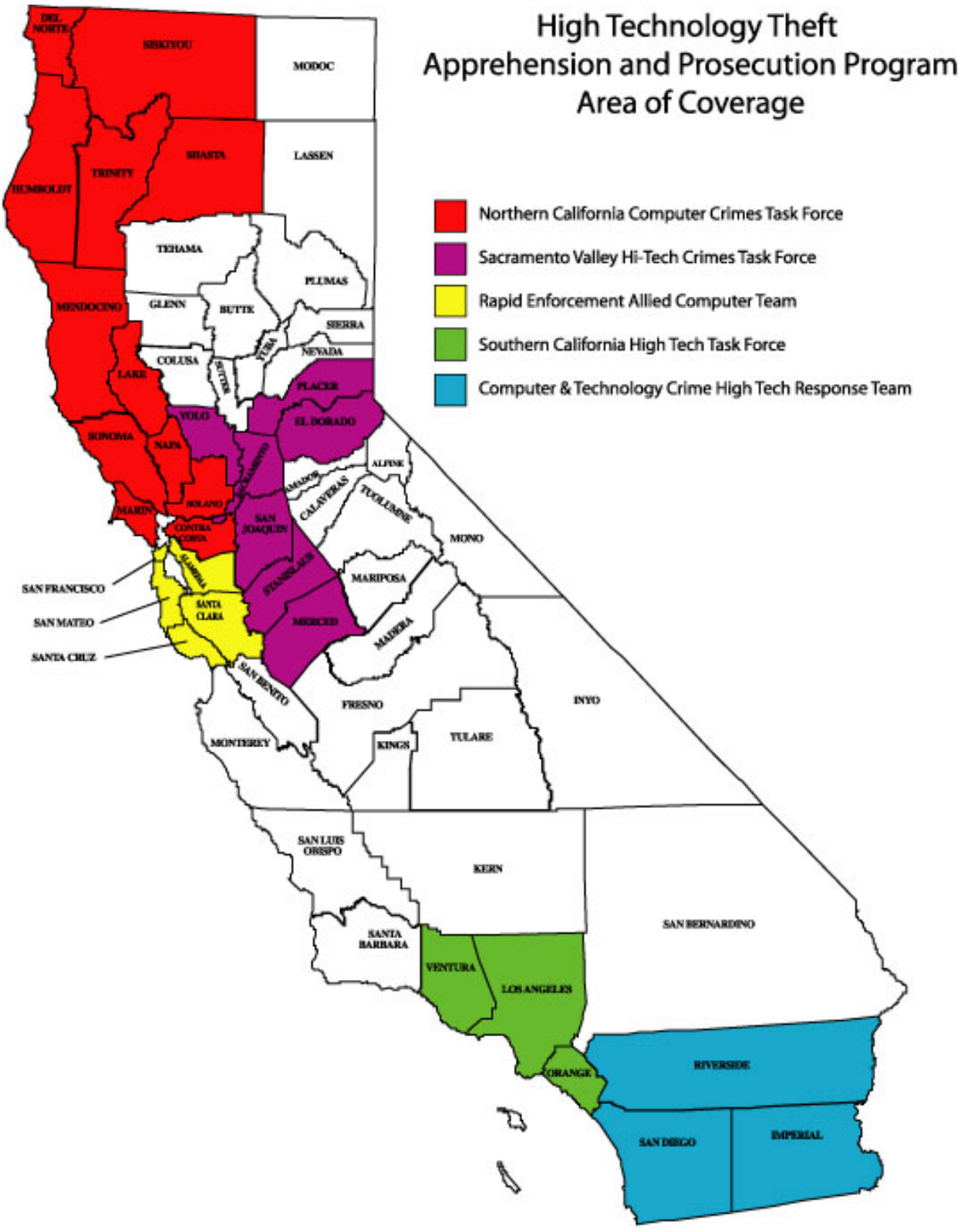
Section 1.

Amendments to these bylaws may be proposed by a Committee member in writing to all members of the Committee and will be considered at the next regular Committee meeting following the meeting at which the proposed amendment is presented. A two-thirds majority vote of the members present is required to adopt an amendment. An approved amendment shall be effective immediately.

ARTICLE XXII: SUSPENSION OF THE BYLAWS

Section 1.

These bylaws may be suspended by a two-thirds vote of the members of the Committee present if a quorum is present.


High Technology Theft
Apprehension and Prosecution Program
Area of Coverage
Northern California Computer Crimes Task Force
Sacramento Valley Hi-Tech Crimes Task Force
Rapid Enforcement Allied Computer Team
Southern California High Tech Task Force
Computer & Technology Crime High Tech Response Team
DEL NORTE
SISKIYOU
MODOC
HUMBOLDT
TRINITY
SHASTA
LASSEN
TEHAMA
PLUMAS
MENDOCINO
GLENN
BUTTE
SIERRA
COLUSA
SUTTER
YUBA
NEVADA
LAKE
PLACER
YOLO
EL DORADO
SONOMA
NAPA
SACRAMENTO
ALPINE
AMADOR
CALAVERAS
TUOLUMNE
SOLANO
MARIN
CONTRA COSTA
SAN JOAQUIN
MONO
ALAMEDA
STANISLAUS
MARIPOSA
SAN FRANCISCO
SAN MATEO
SANTA CLARA
MERCED
MADERA
SANTA CRUZ
SAN BENITO
FRESNO
INYO
MONTEREY
KINGS
TULARE
SAN LUIS OBISPO
KERN
SAN BERNARDINO
SANTA BARBARA
VENTURA
LOS ANGELES
ORANGE
RIVERSIDE
SAN DIEGO
IMPERIAL